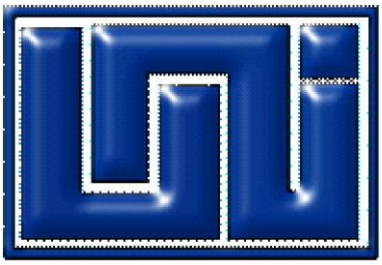
UNIVERSIDAD NACIONAL DE INGENIERÍA

Recinto Universitario Simón Bolívar

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN



"Evaluación de riesgo en las tecnologías de la información en los procesos de facturación de la empresa OCAL S.A

Caso de estudio: Importadora Distribuidora OCAL SA"

Documento Monográfico para obtener el título de Ingeniero en Computación

Tutor:

Msc. Johnny Flores Delgadillo

Presentado por:

Br. Sergio Stewarth Barberena Ruiz 2005-20646

Managua, Febrero 2018

.

I. INDICE

Tabla de contenido

Índice de Ilustraciones

Índice de Tablas

II. RESUMEN DEL TEMA

En este trabajo se aborda **la Evaluación de riesgo en las tecnologías de la información en los procesos de facturación de la empresa OCAL S.A**, haciendo uso de la norma internacional para la gestión de riesgo ISO 3100-2009. Para la presentación del informe se utilizará el método de investigación **CASO DE ESTUDIO.**

III. INTRODUCCIÓN

El uso de tecnologías de la información en las organizaciones sin importar el giro de negocio se ha intensificado al largo de los últimos años, evolucionando, acoplándose a las necesidades y siendo parte de la operación diaria. Lo que ha provocado que sea necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información (Castro, 2017).

La empresa OCAL S.A es una empresa importadora distribuidora de productos varios como: Alimentos, snacks (bocadillos), bebidas, artículos uso doméstico personal, vinos, licores y productos de farmacia, con presencia en todos los departamentos de Nicaragua, actualmente cuenta con dos CEDI[1] , el CEDI Central ubicado en Nindiri y el CEDI Norte ubicado en Sebaco en el departamento de Matagalpa.

Con el crecimiento de sus operaciones, y la adopción de tecnologías de la información en los procesos críticos (facturación, logística, financieros, comunicaciones, etc…) surge la necesidad analizar e identificar riesgos que puedan afectar los bienes informáticos y por ende afectar sus operaciones.

La entidad encarga administrar y adquirir los bienes informáticos y de comunicaciones, la Gerencia de Tecnología de la información y comunicaciones (Gerencia de TIC), vela por la continuidad de las operaciones.

El presente estudio monográfico se enfoca en el análisis de riesgos tecnológicos en el proceso de facturación de la empresa OCAL S.A. Utiliza la metodología de investigación “Caso de estudio”, para la recopilación de la información detallada del área de estudio y de la unidad en análisis, alineada la norma internacional para la gestión de riesgo ISO 31000:2009, la cual proporciona directrices para gestionar el riesgo que servirá como un fuerte fundamento para la toma decisiones con respecto al tratamiento del riesgo.

[1] CEDI: Centro de distribución inteligente

IV. OBJETIVOS

1. OBJETIVO GENERAL

Evaluar los riesgos en las tecnologías de la información que soportan el proceso de facturación de la empresa OCAL S.A.

2. OBJETIVOS ESPECÍFICOS

- Alinear la evaluación de riesgo al estándar internacional de la administración de riesgo ISO 31000:2009.
- Diseñar y Conducir un caso de estudio en base a las consideraciones teóricas pertinentes.
- Analizar el proceso de facturación en base a una matriz de riesgo aplicando Norma IEC/FDIS 31010 para la gestión de riesgo.

V. ANTECEDENTES

Anteriormente no existen estudios realizados de análisis de riesgos en las tecnologías de la información hechos en la empresa OCAL S.A. Sin embargo, la gerencia de tecnología de la información y comunicaciones (TIC), con lo que cuenta actualmente es con un PLAN DE CONTINGENCIAS INFORMATICAS, el cual es una guía en la cual se definen procedimientos a seguir en caso de eventos graves en las tecnologías de la información que soportan las operaciones críticas de la empresa.

VI. JUSTIFICACION

La presente monografía se realiza porque actualmente no existen estudios de análisis de riesgos sobre los bienes informáticos que soportan los procesos críticos de la compañía OCAL SA, y se desconocen efectos negativos que podría tener sobre los procesos críticos de la compañía, en este caso enfocado en el proceso de facturación.

La compañía ha expandido sus operaciones de facturación a lo largo del territorio nacional, en sus 80 años de existencia, esto ha provocado que la información que se genera se haya incrementado y que los procesos facturación se hayan diversificado.

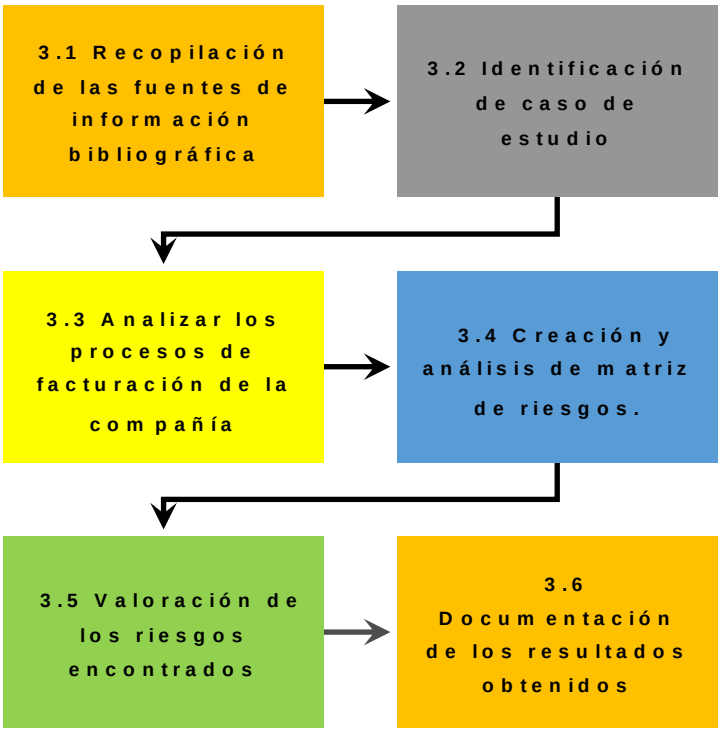
Por tal motivo la gerencia general desea tener un mejor control de la información y de los procesos de facturación en todo momento, para esto ha incorporado las tecnologías de la información; con el apoyo de la gerencia de tecnología la cual ha creado, adquirido y adaptando las tecnologías información, tales como equipos de cómputo, smartphones, servicios de almacenamiento en la nube, internet corporativo, infraestructura de red, etc. para poder cumplir con las metas propuestas.

Dicha incorporación ha generado grandes beneficios (mejor control de la información, procesos y disponibilidad 24/7) pero también riesgos que pueden entorpecer e impedir con el cumplimiento de las metas de la compañía, por tal motivo la gerencia de tecnología ha solicitado realizar un análisis de riesgos para poder identificar y atacar dichos riesgos enfocándose en unos de sus procesos críticos el cual representa su principal giro como negocio, en este caso el proceso de facturación.

VII. MARCO TEÓRICO

3. DISEÑO METODOLÓGICO.

Ilustración 1 Diseño Metodológico



Las etapas principales por las cuales se va elaborar el estudio son los siguientes:

La Ilustración 1 representa las fases que están presentes en el diseño metodológico

3.1 Recopilación de las fuentes de información bibliográfica: El propósito de esta fase es la fundamentación teórica de la tesis.

3.2 Identificación de caso de estudio: Se establece el caso en la empresa Importadora Distribuidora OCAL S.A, que tiene como giro principal de negocios la venta, importación y distribución de productos de distintas marcas en el territorio nacional, y requiere un análisis de riesgos tecnológicos en los procesos de facturación que se llevan a cabo.

3.3 Analizar los procesos de facturación de la compañía: En base a las tecnologías de la información que la soportan dichos procesos.

3.4 Creación y análisis de matriz de riesgos: Establece la identificación, ponderación y análisis de los riesgos asociados con los procesos de facturación.

3.5 Valoración de los riesgos encontrados: En esta fase se procederá a valorar los riesgos.

3.6 Documentación de los resultados obtenidos.

4. RIESGO TECNOLÓGICO.

Antes de ahondar en la definición de riesgo tecnológico es importante conocer la definición del **riesgo**. Según la ISO 3100:2009, es el efecto de incertidumbre de poder alcanzar las metas u objetivos debido a eventos internos o externos por tal motivo se define, el **riesgo tecnológico** a todos aquellos eventos que amenacen a los bienes o servicios informáticos que soportan los procesos críticos en una organización y que provoquen que los objetivos de esta no sean cumplidos.

Ahora bien, al análisis de ocurrencia de eventos internos y externos que puedan provocar la incertidumbre en el alcance de los objetivos se le llama **análisis de riesgos**. El análisis de riesgos trata de desarrollar una comprensión del mismo, para lo cual se proporciona una entrada, se evalúa y se toman las decisiones para su tratamiento. Sobre dicho análisis, es que se desarrollan estrategias o métodos para su mitigación.

Los métodos utilizados para analizar los riesgos pueden ser cualitativos, semi-cuantitativos o cuantitativos. La evaluación cualitativa define la consecuencia, la probabilidad y el nivel de riesgo por significación Niveles tales como "alto", "medio" y "bajo", pueden combinar consecuencia y probabilidad, y evalúa el nivel de riesgo resultante con respecto a criterios cualitativos.

5. PROCESO DE GESTION ISO 31000: GESTION DE RIESGO Y ANALISIS DE RIESGO TI.

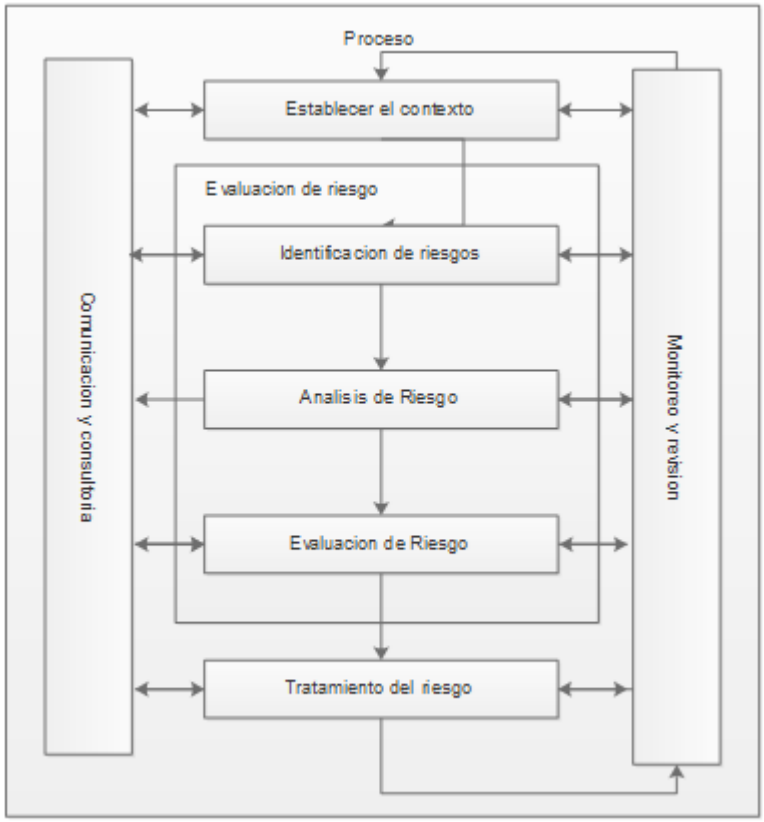
ISO, la Organización Internacional de Estandarización, es una organización independiente y no-gubernamental formada por las organizaciones de estandarización de sus 164 países miembros. Es el mayor desarrollador mundial de estándares internacionales voluntarios y facilita el comercio mundial al proporcionar estándares comunes entre países. Se han establecido cerca de veinte mil estándares

cubriendo desde productos manufacturados y tecnología a seguridad alimenticia, agricultura y sanidad.

La norma ISO 31000:2009 establece una serie de principios que deben ser satisfechos para hacer una gestión eficaz del riesgo. Esta norma internacional recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte (framework[2]) cuyo objetivo es integrar el proceso de gestión de riesgos en el gobierno corporativo de la organización, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura. En la Norma **ISO 31000:2009**, se usan las expresiones "gestión del riesgo" y "gestionar el riesgo". En términos generales, la "gestión del riesgo" se refiere a la arquitectura (principios, marco de referencia y procesos) para la gestión eficaz del riesgo, mientras que "gestionar el riesgo" se refiere a la aplicación de esa arquitectura a riesgos particulares.

[2] Framework es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

Ilustración 2 Proceso de gestión de riesgos



La ilustración 2 a continuación se reproduce desde el AS / NZS ISO 31000, representa la relación entre los principios que sustentan la gestión del riesgo, el marco de gestión de riesgos, y el proceso de gestión de riesgos. Según la ISO 31000:2009, el proceso de gestión de riesgos consiste en siete pasos:

Paso 1: Establecimiento del contexto: Determina los límites dentro de los cuales el marco de gestión de riesgos operará. Tomando en consideración el marco y la capacidad del organismo para hacer frente con éxito a los riesgos que pueden ser identificados en la fase de evaluación del proceso. Para posteriormente establecer entorno externo e interno de la organización.

Las principales influencias sobre el medio ambiente externo se refieren a los entornos sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos y económicos en los que opera la compañía. Estas influencias externas podrían

ocurrir a niveles regionales o locales internacionales, nacionales, estatales. Influencias en el ambiente interno pueden incluir:

1. Objetivos de la compañía y los resultados previstos

2. Planes establecidos para asegurar que la agencia logra sus objetivos y ofrece sus servicios

3. Proyectos individuales que están siendo llevadas a cabo por la agencia

4. Estructuras de gobierno y rendición de cuentas de la agencia

5. Las políticas establecidas por el organismo

6. Los recursos disponibles dentro del organismo (por ejemplo, sistemas de información, de personal y de financiación), y

7. Conocimientos y prácticas de gestión del riesgo existente.

Los ambientes externos e internos definidos deben ser examinados regularmente y sistemáticamente para asegurar que siguen siendo apropiado y deseable.

Paso 2. Identificación de Riesgos. El objetivo de este paso es generar una lista completa de las amenazas y oportunidades basadas en esos eventos que podrían crear, mejorar, prevenir, degradar, acelerar o retardar la consecución de los objetivos estratégicos de la compañía. La identificación integral es crucial, ya que el riesgo de que no se identifica en esta etapa no será incluido en el análisis adicional. Al identificar el riesgo, tenga en cuenta estos tipos de preguntas: ¿Lo que puede suceder y por qué (por la identificación de riesgos)? ¿Cuáles son las consecuencias? ¿Cuál es la probabilidad de su ocurrencia futura? ¿Existen factores que mitigan la consecuencia del riesgo o que reducen la probabilidad del riesgo?

Paso 3. Análisis de Riesgos. Una vez que el riesgo ha sido identificado y el contexto, las causas, los factores contribuyentes y las consecuencias han sido descrito, mirar las fortalezas y debilidades de los sistemas y procesos existentes diseñados para

ayudar a controlar el riesgo. Identificar los controles existentes - determinar qué controles son ya previstas para mitigar el impacto del riesgo. Los controles pueden ser fuertes o débiles; pueden ser medible y repetible. Los controles pueden incluir legislación, políticas o procedimientos, formación del personal, la separación de funciones, personales medidas y equipos de protección y estructural o barreras físicas

Paso 4. Evaluación de los riesgos. Una vez que se han identificado y evaluado los riesgos, se debe determinar cuáles son los riesgos a tratar y la prioridad para la aplicación del tratamiento. Este proceso se conoce como la evaluación de riesgos.

Paso 5. Tratamiento de los riesgos. Una vez que los riesgos han sido analizados y evaluado, se necesita evaluar el tratamiento apropiado de los riesgos

Paso 6. Propuesta de monitoreo y revisión. El continuo y revisión son componentes vitales en un efectivo proceso de gestión de riesgos. El propósito primario del monitoreo y revisión es determinar si existen o subsisten los riesgos, si nuevos riesgos han surgido, si la probabilidad o el impacto de los cambios en los riesgos, y revaluar las prioridades de riesgo dentro del contexto interno y externo de la compañía.

Paso 7. Comunicación y consulta. La comunicación, la consulta y la información periódica deben tomar durante todas las etapas del proceso de gestión de riesgos. La naturaleza del riesgo (por ejemplo, estratégica, operativa, política) tendrá que ser considerados en la determinación de un proceso de consulta adecuado.

Para la presente monografía los pasos 6 y 7 no se usan para el desarrollo del mismo, pero se mencionan ya que son parte del proceso de gestión de riesgo.

6. MODELO DE MATRIZ DE RIESGO.

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más

importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

Debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de una entidad. Exige la participación activa de las unidades de negocios, operativas y funcionales en la definición de la estrategia institucional de riesgo de la empresa.

Una efectiva matriz de riesgo permite hacer comparaciones objetivas entre proyectos, áreas, productos, procesos o actividades. Todo ello constituye un soporte conceptual y funcional de un efectivo sistema Integral de gestión de riesgo

La matriz de riesgo permite establecer de un modo uniforme y consistente el perfil de riesgo de cada una de las entidades y permite profundizar en el proceso de establecimiento de planes de supervisión a fin de que se ajusten a las características específicas de cada entidad.

6.1 CONSTRUCCIÓN DE MATRIZ DE RIESGO

Ahora que se abordado las generalidades de una matriz procederemos a construirla, para esto tendremos los siguientes puntos en cuenta:

1. Se debe desarrollar un proceso para la “identificación “de las actividades principales y los riesgos a los cuales están expuestas.
2. Identificar las fuentes o factores que intervienen en su manifestación y severidad, es decir los llamados “factores de riesgo”
3. Determinar la “probabilidad” de que el riesgo ocurra.

4. Posteriormente realizar un cálculo de los efectos potenciales sobre el capital o las utilidades de la entidad al cual llamaremos impacto de riesgo, este considera lo que pido haber sucedido, así como lo que realmente ocurrió.
5. Evaluar el riesgo implica un análisis combinado de la probabilidad de ocurrencia del riesgo y el efecto de los resultados, puede efectuarse en términos cuantitativos o cualitativos esto dependerá de la importancia y disponibilidad de información. Las estimaciones cualitativas y cuantitativas pueden complementarse en el proceso del trabajo de estimar la probabilidad de riesgo.

Para implementar una matriz de riesgo debemos establecer los criterios bajo los cuales se van a regir los datos que se van a introducir y los datos que la matriz como resultados.

Primero se diseñan los criterios de probabilidad, esto podemos realizarlos apoyados en una tabla de criterios de probabilidad.

Tabla 1 Criterios de Probabilidad

Calificación	Puntuación	Descripción
Casi seguro	**5**	**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**
Probable	**4**	**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**
Posible	**3**	**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**
Improbable	**2**	**Xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**
Raro	**1**	**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx**

La tabla 1 es un ejemplo de cómo se debe de construir una tabla de criterios de probabilidad en este debe se deben colocar la clasificación del riesgo, la puntuación del riesgo esto en base al criterio que se va a utilizar y la descripción de los riesgos

A continuación, se presentan las leyendas de la tabla de criterios de probabilidad:

Clasificación: Clasificación de la probabilidad.

Puntuación: La valorización de la probabilidad.

Descripción: sólo indicativos y proporcionan una guía para consecuencia relativa

Luego se diseñan los criterios de impacto de riesgo, esto podemos realizarlo apoyando creando una tabla de criterios de impacto.

Tabla 2 Criterios de impacto de riesgo

Clasificacion	Puntuación	Criterios
Catastrofico	5	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Grave	4	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Moderado	3	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Menor	2	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Insignificante	1	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

La tabla 2 es un ejemplo de cómo se debe construir una tabla de impacto de riesgo, aquí se debe de colocar la clasificación del impacto de riesgo, la puntuación que se le va a asignar y la descripción del criterio.

A continuación, se presentan las leyendas de criterios de impacto

Clasificación: Clasificación del impacto del riesgo.

Puntuación: La valorización del impacto del riesgo.

Descripción: Sólo indicativos y proporcionan una guía para impacto del riesgo.

Posteriormente de acuerdo a los riesgos obtenidos los colocaremos en una tabla de riesgos como la presentada en la ilustración 3, para luego poder ubicarlos en una matriz de riesgos.

Ilustración 3 Tabla de riesgos

TABLA DE RIESGOS		
RIESGOS	PROBABILIDAD	IMPACTO

A continuación, se presentan matriz de evaluación de riesgo a como se presenta en la ilustración 4

Ilustración 4 Matriz de evaluación de riesgo

			GRAVEDAD (IMPACTO)			
			BAJO	MEDIO	ALTO	CRITICO
			1	2	3	4
Frecuencia (probabilidad)	ALTA	**4**				
	MEDIA	**3**				
	MUY BAJA	**2**				
	BAJA	**1**				

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente aj es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

En esta matriz se clasificará el riesgo en función de las puntuaciones de consecuencia y probabilidad, los riesgos serán ubicados de acuerdo en función de la intercepción que haya entre la consecuencia y probabilidad de ocurrencia del riesgo.

Posteriormente se diseñan los criterios de acciones requeridos estos en base a la clasificación de los riesgos.

Tabla 3 Criterios de acción de riesgos

Nivel de riesgo	Acción requerida
CRITICO	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.
ALTO	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
MEDIO	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
BAJO/MUY BAJO	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

La tabla 3 es un ejemplo de cómo se debe construir una tabla criterios de acción de riesgo, el nivel de riesgo en base a su clasificación y la acción requerida, en el caso de las acciones a tomar estas son en bases a las necesidades y/o prioridades de las organizaciones.

A continuación, se presentan las leyendas de criterios de acción de riesgo.

Nivel de riesgo: Clasificación del riesgo

Acción requerida: Plazos de tiempo para asegurarse de que se eliminan los riesgos.

7. TÉCNICA DE ESTUDIO DE CASO

El **caso de estudio** es un instrumento o método de investigación con origen en la investigación médica y psicológica. Se sigue utilizando en áreas de ciencias sociales como método de evaluación cualitativa (Becker).

En cuanto a los objetivos del caso de estudio, trata:

- Producir un razonamiento inductivo. A partir del estudio, la observación y recolección de datos establece hipótesis o teorías.
- Puede producir nuevos conocimientos al lector, o confirmar teorías que ya se sabían.
- Hacer una crónica, un registro de lo que va sucediendo a lo largo del estudio.
- Describir situaciones o hechos concretos

- Proporcionar ayuda, conocimiento o instrucción a un caso estudiado
- Comprobar o contrastar fenómenos, situaciones o hechos.
- Pretende elaborar hipótesis.

Es decir, el caso de estudio pretende explorar, describir, explicar, evaluar y/o transformar.

7.1 RECOLECCIÓN DE DATOS

Para Yin[3] las interrogantes de investigación o preguntas de estudio, son el primer elemento del diseño de cualquier investigación. Estas interrogantes identifican el problema central de la investigación e indican qué metodología de investigación será la más adecuada. Según este autor las interrogantes "cómo" y "por qué" son los más indicados para una metodología de caso de estudio. A continuación, sus métodos:

• Recolección de datos: los métodos más utilizados para la recolección de datos en las investigaciones cualitativas por lo general, y el caso de estudio en particular, son la observación, la entrevista y el análisis de documentos. Yin establece hasta seis métodos de obtención de datos o "fuentes de evidencias", como él lo denomina: documentación, documentos de archivo, entrevistas, cuestionarios, observación directa, observación participante y objetos físicos. Aun así, se pueden resumir en los tres tipos antes apuntados puesto que los documentos de archivo, los objetos físicos, los papeles personales y las fotografías se pueden considerar dentro del apartado de documentos. Primordialmente cuestionarios y entrevistas

• Análisis de datos e interpretación de los resultados: es necesario especificar previamente al desarrollo de la investigación cómo se relacionarán los datos obtenidos con las proposiciones o hipótesis definidas y qué criterios serán utilizados para interpretar los resultados.

[3] Es un científico social estadounidense y presidente de COSMOS Corporation, conocido por su trabajo en la investigación de estudios de casos

VIII. CASO DE ESTUDIO.

8. DISEÑO DEL CASO DE ESTUDIO

El diseño del estudio de caso se realizará en base a los pasos descritos del proceso de gestión de riesgo.

En la selección del caso de estudio se establece la Empresa Importadora Distribuidora OCAL SA, que tiene como giro principal de negocio la importación, distribución y venta de productos de distintas marcas a lo largo y ancho del territorio nacional, el estudio de se centrara en el proceso de facturación de la compañía.

Las preguntas a continuación:

1. ¿Cuáles son los objetivos/metas definidos por la organización?
2. ¿Cuál es el giro del negocio en que desarrolla la organización o compañía?
3. ¿Cuáles son los objetivos de la Gerencia de ventas de la compañía?
4. ¿Cómo la organización articula sus objetivos/metas con las unidades organizacionales?
5. ¿Cuáles son las tecnologías de la información asociadas a los procesos de facturación de la compañía?
6. ¿Cuáles son objetivos del de la Gerencia de Tecnología e información?
7. ¿Cuáles son las funciones del área de soporte técnico?
8. ¿Cuáles son las funciones del área de desarrollo de integración y sistemas?
9. ¿Cuáles son los riesgos de las tecnologías de la información asociadas con los procesos de facturación?
10. ¿Cuáles son las causas y posibles consecuencias de los de las tecnologías de la información asociadas con los procesos de facturación?
11. ¿Cuál es la probabilidad de ocurrencia de los riesgos?

12. ¿Cómo se identifican los riesgos de las tecnologías de la información asociadas con los procesos de facturación?
13. ¿Cuáles son las fuentes de los riesgos de las tecnologías de la información asociadas con los procesos de facturación?
14. ¿Qué roles (cargos) están definidos en la Gerencia de Tecnología e información?
15. ¿Cómo se define la carga en la Gerencia de Tecnología e información?
16. ¿Cuál es el origen de estos riesgos?
17. ¿Qué consecuencias resultan de estos riesgos?
18. ¿En un mes con qué frecuencia ocurren estos riesgos?

Las preguntas descritas anteriormente tienen el objetivo de establecer aspectos tales como el contexto y la valoración de riesgo.

En el caso de las fuentes de información, en conjunto con la gerencia de tecnologías y comunicaciones se identificarán los informantes claves de la organización para la obtención de información relevante en el estudio

Las características que debe de poseer el personal participante debe de cumplir con tres o más de las siguientes cualidades a continuación:

1. El participante debe de tener 2 o más años estar laborando en la compañía.

2. Debe de hacer uso de las herramientas tecnológicas (sistemas informáticos, insumos tecnológicos), para el desempeño de sus labores.

3. Debe estar familiarizado o estar involucrado directamente con los procesos de facturación de la compañía.

4. Integrante de la Gerencia de Tecnología y comunicaciones.

5. Integrante de la Gerencia de Ventas.

6. Debe de conocer las tecnologías asociadas con los procesos de facturación de la compañía

A continuación, se presentan los posibles informantes claves en base a las cualidades y criterios que debe de cumplir un entrevistado.

Personal de Informática

- Jefes de departamentos
- Técnicos de Áreas

Personal de Ventas

- Personal de Ventas

Las entrevistas a los informantes claves de la organización se dividirán en tres bloques el primer bloque de entrevista es una reunión general con los jefes de departamento y el gerente de tecnologías y comunicaciones de la compañía. El segundo bloque de entrevistas es con los técnicos de áreas de ventas empresa y el tercer bloque se realizarán con los usuarios finales de los ejecutivos de ventas.

La duración de las Entrevistas con el personal de ventas de ventas se lleva a cabo en un periodo de una hora los días viernes ya que es el día que regresan a la empresa, de igual manera se establecerán entrevistas con el personal de informática en conjunto se revisaran los casos que se han presentado de incidentes con la infraestructura tecnología y sistemas de la información de la compañía de los cuales tengan conocimiento.

Se solicitará información de documentada de todo el proceso de facturación, también información de las tecnologías utilizadas en el proceso de facturación de la compañía, y documentación que pueda ser de utilidad para el desarrollo del Caso de estudio. De acuerdo al resultado de las entrevistas realizadas al personal clave involucrados en el proceso de facturación de la empresa y la revisión de la documentación que se revise, se establecerán los riesgos definir las causas, consecuencias, frecuencia y magnitud de ocurrencia de dichos riesgos.

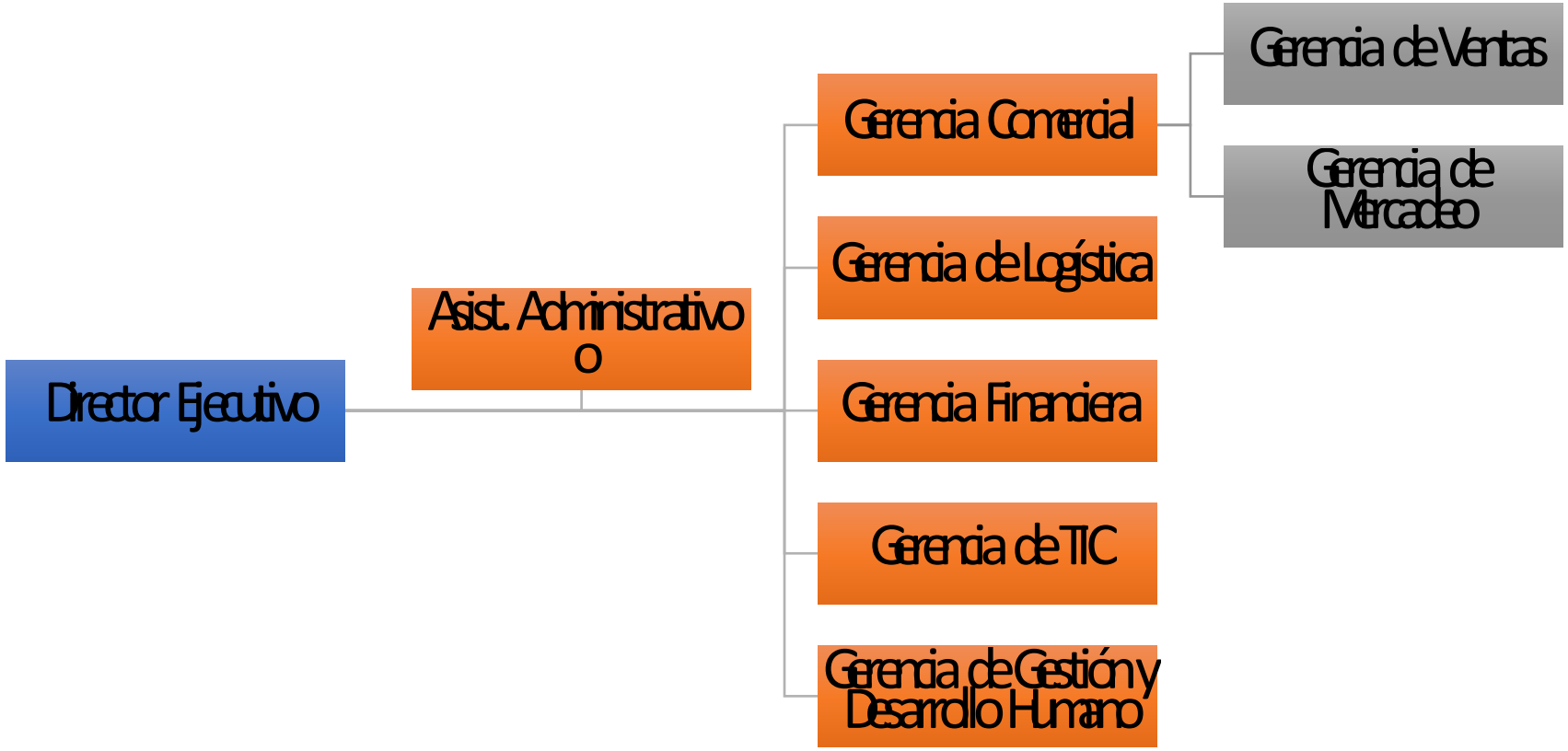
Los criterios de magnitud y frecuencia de los riesgos serán establecidos en conjunto con la Gerencia de tecnología y comunicaciones de la compañía, luego la información será procesada en una matriz de riesgo (Ver sección 3.2), para su evaluarla y cuantificarla de tal manera que se tomen decisiones de cómo se van a tratar los riesgos.

9. CONDUCCIÓN DEL CASO DE ESTUDIO

9.1 ESTRUCTURA ORGANIZATIVA

Se hará el análisis de riesgo sobre el proceso de facturación de OCAL S.A. Dicha compañía cuenta con una gerencia de tecnología que se encarga de velar por los bienes tecnológicos de la misma. La estructura organizativa de la compañía se muestra a continuación:

Ilustración 5 Estructura Organizativa de la empresa OCALSA



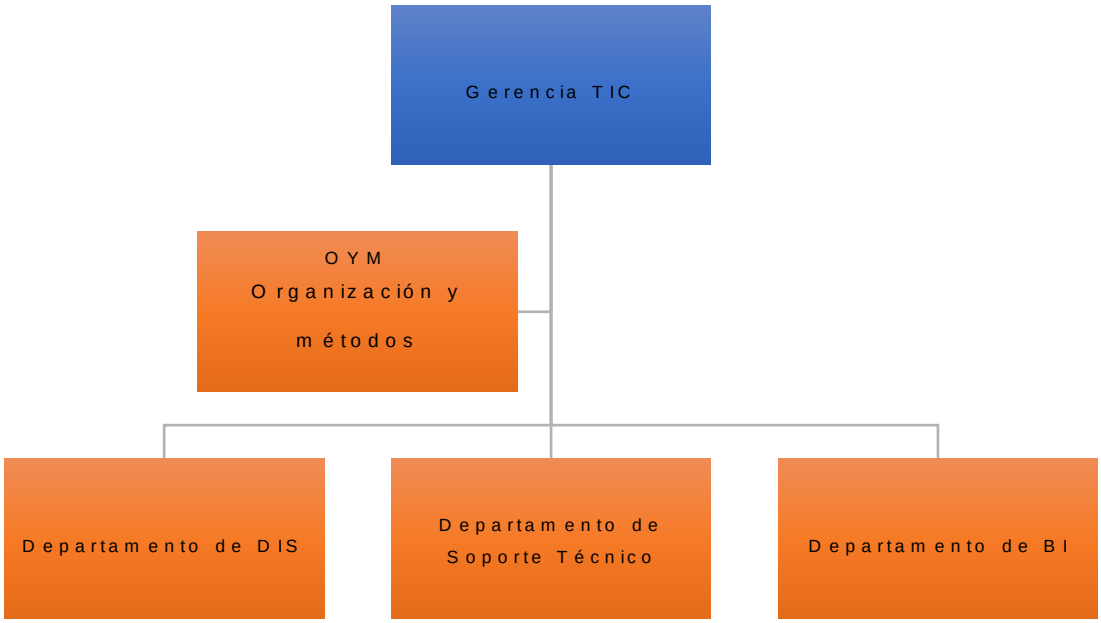
9.1.1 Gerencia de Tecnología y comunicaciones (TIC):

Tiene como objetivo principal el apoyo al resto de áreas, para garantizar que las operaciones de la empresa sean ágiles, confiables y seguras, utilizando para ello tecnología de punta, tanto en Hardware como en Software. Además, administrar todos los recursos informáticos (humanos, técnicos) para que la empresa logre sus metas a corto, mediano y largo plazo.

Así mismo trabaja en:

- Planificar, administrar y dar seguimiento a las estrategias a corto y largo plazo del crecimiento informático de la empresa
- Planificar y coordinar las estrategias de capacitación orientadas al personal técnico y a usuarios de aplicación, en conjunto con la Gerencia de Recursos Humanos
- Administrar todos los recursos informáticos (humanos y técnicos) a disposición de la empresa
- Dirigir el diseño y desarrollo de nuevas aplicaciones
- Definir procedimientos y controles a nivel de Software y Hardware para evitar los riesgos de pérdida de información por: Robo, manejo indebido por parte de usuarios, acceso no autorizado a nuestra base de datos, desastre natural y otros.
- Garantizar el funcionamiento de todos los medios informáticos que se utilizan para apoyar todas las operaciones de la empresa.
- Elaborar planes de contingencias ante cualquier desastre natural o político, con el objetivo de asegurar que las operaciones diarias de la empresa no se detengan
- Proponer a la Dirección de la empresa nuevos proyectos tecnológicos alineados a los planes estratégicos de la empresa
- Elaborar y administrar el presupuesto anual de tecnología de la empresa.

Ilustración 6 Diagrama organizacional de la gerencia de tecnología y comunicaciones



La ilustración 6 presenta la estructura organizativa de la gerencia de tecnología y comunicaciones, aquí se presentan cuales son todas las áreas que se encuentran bajo la tutela directa de la gerencia de tecnología, las cuales son Organización y métodos (OYM), departamento de desarrollo e Integración y sistemas (DIS), departamento de soporte técnico y departamento de Inteligencia de negocios (BI)

Tabla 4 Estructura de la Gerencia de TIC

Encargado:	Personal a Cargo	
Msc. Javier Cordero	**Colaboradir**	**Puesto**
	Ing. Jared Gómez	Jefe DIS
	Ing. Saul Potosme	Jefe Soporte Técnico
	Ing. Marlon Avilés	Analista de OYM

La Tabla 4 representa la estructura representa los Jefes de departamento que se encargan de la dirección de cada una de las áreas de la Gerencia de Tecnología y comunicaciones

9.1.2 Departamento de Soporte Técnico:

Es el departamento encargado del correcto funcionamiento y mantenimiento de la estructura física y virtual de la intranet y servidores de la compañía en todos los CEDI, así como de los distintos dispositivos utilizados por los usuarios finales de la compañía como: computadoras, handhelds, Smartphone, impresoras, routers y sistemas operativos.

Otra de las tareas que lleva el área de soporte técnico es brindar soluciones en el caso de incidentes relacionados con la estructura física, virtual y de los dispositivos usados por los usuarios finales.

Así mismo colabora en:

- Apoyar los objetivos del Departamento de Sistemas, en la administración, adquisición y mantenimiento de todos los medios de hardware necesarios para trabajar con los Sistemas Informáticos de la empresa
- Administrar todos los recursos tecnológicos de la empresa bajo la supervisión de la Gerencia TIC
- Dar mantenimiento preventivo de forma oportuna a los equipos informáticos de la empresa
- Hacer cumplir las políticas y procedimientos de seguridad establecidos para el control de los equipos informáticos
- Apoyar a la Gerencia TIC en la definición de estrategias para el crecimiento en la infraestructura tecnológica.

Tabla 5 Estructura del Dpto. Soporte Técnico

Encargado:	Personal a Cargo	
Ing. Saul Potosme	**Persona**	**Puesto**
	Ing. Yader Bendaña	Auxiliar de Soporte Técnico A
	Ing. Norman Arévalo	Auxiliar de Soporte Técnico B

La Tabla 5 representa los integrantes que se encuentran en el departamento de soporte técnico.

9.1.3 Departamento de Desarrollo e Integración de Sistemas

Es el departamento encargado del correcto funcionamiento y mantenimiento de los distintos sistemas, bases de datos que se utilizan en los distintos departamentos de la compañía en todos los CEDI, así como el encargado de realizar desarrollos de nuevos sistemas y la supervisión de la implementación e implantación de nuevos sistemas en la compañía, además de atender incidentes relacionados con los sistemas de la compañía.

Otra de las tareas del departamento es brindar soluciones en el caso de incidentes relacionados con los sistemas, bases de datos de la compañía. Así mismo se encarga de:

- Apoyar a las distintas áreas de la empresa con herramientas informáticas de software con el objetivo de agilizar los procesos diarios de la empresa, además de resguardar y asegurar la información almacenada.
- Administrar y asegurar el buen funcionamiento de todos los Sistemas Informáticos que operan en la empresa.
- Desarrollar nuevos proyectos tecnológicos alineados con el plan estratégico de la empresa
- Asegurar la información de la empresa definiendo políticas de seguridad.

Tabla 6 Estructura del Dpto. DIS

Encargado:	Personal a Cargo	
Ing. Jared Gómez	**Personal**	**Puesto**
	Mario Zúñiga	Analista de Sistemas
	Ing. Harriete Martinez	Analista de Sistemas
	Sergio Barberena	Analista de Sistemas
	Ing. Martha Vividea	Analista de Sistemas

La tabla 6 representa a los integrantes del departamento del desarrollo e integración de sistema.

9.1.4 Departamento de Inteligencia de Negocios (Bussines Inteligence)

Es el departamento encargado de administrar los productos y servicios que permiten a los usuarios finales acceder y analizar de manera rápida y sencilla, la información para la toma de decisiones de negocio a nivel operativo, táctico y estratégico.

- Administrar los recursos de información de la empresa (internos y externos).
- Promover estrategias para la implementación de soluciones BI.
- Promover la cultura de información a todos los niveles de la empresa.
- Dar mantenimiento continuo a las soluciones de usuario final del BI.
- Coordinar el desarrollo de proyectos de inteligencia de negocios.

Tabla 7 Estructura del Dpto. BI

Encargado:	Personal a Cargo	
Msc. Javier Cordero	**Personal**	**Puesto**
	Ing. Arlen López	Analista BI
	Brenda Sánchez	Analista BI

La Tabla 7 representa a los integrantes del departamento del departamento de inteligencia de negocios.

9.1.5 Organización y Métodos (OYM)

- Administrar los procesos internos de la organización.
- Desarrollar políticas y normativas en la definición de procesos.
- Elaborar y documentar nuevos procesos.
- Mejora continua de los procesos ya creados.
- Realizar reingeniería de procesos cuando se requiera.
- Dar seguimiento al cumplimiento de los procesos.
- Capacitar a los usuarios involucrados en los procesos.
- Elaboración de manuales de usuarios o guías de procesos.
- Publicar debidamente los procesos aprobados.

Tabla 8 Estructura OYM

Encargado:	Personal a Cargo	
	Personal	**Puesto**
Msc. Javier Cordero	Ing. Marlon Avilés	Analista OYM

La tabla 8 representa a los integrantes del área de organización y métodos.

9.1.6 Gerencia de Ventas

Tiene como objetivo principal el mantener y aumentar las ventas, mediante la administración eficiente del recurso humano de venta disponible y del mercado potencial de clientes en un plazo determinado.

Desacuerdo a la Gerencia de ventas, la compañía en un mes de trabajo puede llegar a vender los 3,000,863.53 de Dólares, el monto de venta puede ser variable y puede cambiar de acuerdo a la temporada del año, por ende, se estima que el monto de venta en un día de trabajo es de 115,417.828 Dólares en una jornada laboral sin contratiempos, trabajando 26 días al mes en una jornada de 8 horas, por lo tanto, en una hora puede vender 14,427.2285 Dólares, esto con el apoyo de 73 ejecutivos de ventas o asesores de ventas, en una hora se estima que 1 ejecutivo puede vender 197.63 dólares.

Como parte de las estrategias que plantea la gerencia de ventas para cumplir con las metas propuestas por la dirección ejecutiva de la compañía, la gestión de ventas está divida de la siguiente manera:

Canal Detalle: Están dirigidos al sector de los pequeños comercios como pulperías o pequeños negocios. El esquema de ventas es el de Preventa. Cuenta con un total de 52 ejecutivos de ventas.

Para la facturación el asesor de ventas levanta la orden con los productos solicitados por los clientes, y estos son entregados en la fecha establecida por los clientes no

mayor a siete días, en el caso de que el cliente requiera que el producto sea entregado posterior a los siete días.

Canal Mayorista: Está dirigido en atender las necesidades de los clientes y/o comerciantes que venden al por mayor, tales como distribuidoras en los distintos mercados del país. el esquema de ventas es el de Preventa. Cuenta con un total de 4 Ejecutivos de ventas

Canal Autoservicio: El canal Autoservicio está dirigido a atender a los supermercados, comisariatos, estaciones de servicio. el esquema de ventas es el de Preventa. Cuenta con un total de 4 Ejecutivos de ventas

Canal de Food Services, rutas especiales, Otros: Está orientado en la atención en los hoteles, gasolineras, cines, restaurantes. El esquema de ventas es el de Preventa. En el caso del Canal Food Services y rutas especiales es el esquema de ventas es el de Preventa. Cuenta con un total de 5 Ejecutivos de ventas.

Canal Tele ventas y ventas de oficina: El canal de tele ventas es el canal dirigido a la facturación dentro de las instalaciones de la empresa, en este canal los clientes se dirigen directamente a la compañía y obtiene su producto de inmediato o pueden arreglar que el transporte de la compañía les deje los productos en un lugar según lo indique el cliente, atienden la facturación del personal de la compañía, y se encargan al mismo tiempo conseguir clientes a través de la guía telefónica. Cuenta con 2 ejecutivos de ventas

Canal Zona Libre: El canal de tienda zona libre está dirigido a la tienda que se encuentra en el interior del Aeropuerto Internacional Augusto César Sandino, el régimen de venta directa bajo un régimen sin impuesto. Cuenta con 3 ejecutivos de ventas

Canal Perecedero y Frutas: El canal de perecederos está dirigido en atender las necesidades de clientes que requieren productos perecederos. El esquema de ventas es el de venta directa. Cuenta con 3 ejecutivos de ventas

El personal encargado la venta de los productos de la compañía se le denomina **asesor de ventas o ejecutivo de ventas**, al cual se le asigna una cartera de clientes en una ubicación geográfica y se agenda tiempo de visitas.

La secuencia de visita que los asesores de ventas realizan a sus clientes se le denomina **itinerario de visita.**

Ruta de venta es el conjunto de itinerarios que el vendedor ha de seguir para visitar, periódicamente o no, a los clientes designados.

Todos los canales de manera general están compuestos por:

Supervisor de canal

Supervisar a los vendedores de la empresa y display de Ruta en sus funciones diarias para mejorar los niveles de ventas en el canal detallista Managua o Foráneo. Elaborar un plan de trabajo de campo para la supervisión adecuada que permita detectar oportunidades y debilidades.

- Orientar y dar seguimiento al estricto cumplimiento de las normas y políticas emanadas por la Gerencia de Ventas.
- Coordinar reuniones de evaluación de vendedores detallistas de la empresa.
- Realizar un análisis del informe semanal de cada vendedor en conjunto con el equipo asignado.
- Revisar los viáticos presentados por el equipo de vendedores asignados e ingresarlos en el sistema para su autorización.
- Supervisar en la ruta asignada el trabajo realizado por cada vendedor.
- Recoger continuamente la problemática (incidencias) de los vendedores relacionados con los clientes para asesorarlos.
- Elaborar los reportes de ventas en base a los datos obtenidos de su equipo.

- Dar seguimiento al cumplimiento de cuotas y recuperación de cartera organizando, planificando, apoyando y dirigiendo al personal de ventas a cargo.
- Archivar eventualmente los reportes realizados.
- Brindar una adecuada atención a los clientes en cuanto a sus necesidades y verificar la correcta entrega de los pedidos en tiempo y forma.

Asesores de venta

Optimizar los niveles de distribución y venta efectiva de los productos que oferta OCAL S.A. a través del Canal de Ventas de Detalle.

- Visitar y ofrecer a los clientes en cada pulpería establecida en la ruta los productos que oferta OCAL S.A. para cumplir con la venta efectiva.
- Administrar de manera eficiente la ruta designada.
- Prospectar clientes nuevos en la ruta establecida previamente por el supervisor.
- Remitir al Área de Aseguramiento de Pedidos los requerimientos realizados por los clientes de manera instantáneo vía sistema.
- Regir las ventas a realizar basados en el inventario en línea enviado por el Supervisor Regional.
- Llevar control detallado de las ventas realizadas en el día.
- Informar al Supervisor Regional sobre incidencias ocurridas durante las ventas.
- Administrar el material publicitario y promocional que se utiliza en los puntos de venta.
- Controlar la rotación de la mercadería en las pulperías que ofertan el producto.
- Solicitar la autorización de los clientes para revisar, limpiar o arreglar los productos dentro de las bodegas o almacenes que poseen.
- Revisar y controlar las fechas de los productos o mercadería próximas a vencerse y que sean ofertadas a los clientes.
- Gestionar con los Gerentes de Marca los cambios de productos con defectos de fábrica.

- Realizar cobro efectivo a clientes de la cartera de crédito.
- Administrar el plazo de pago de los clientes a los que se les haya autorizado el crédito.
- Depositar el dinero recaudado por cobro y pagos de los clientes, en el horario establecido en las políticas de la compañía.
- Realizar cualquier otra tarea asignada por el jefe inmediato y que esté acorde a los objetivos de su puesto.

9.1.6.1 Procesos de facturación

Los tipos de ventas que se realizan en la empresa OCAL S.A son los siguientes:

Venta Directa: La venta directa es aquel tipo de venta en el cual se vende directamente al cliente y se le entrega el producto, este tipo de venta por el momento está orientado a los perecederos, en esta modalidad el pago es recibido al momento de facturarse el o los artículos, este se aplica a los canales de perecederos y tienda zona libre

Preventa: En la modalidad de preventa, es aquel tipo de venta en el cual el cliente ordena los productos para luego entregarse según las instrucciones de entrega que el asesor de ventas indique, en esta modalidad el pago es recibido hasta que los productos son entregados a los clientes. En esta modalidad se encuentran los clientes de Canales Mayoristas, Detalle, Food Services, Autoservicios, rutas especiales y otros.

Ventas de oficina: Este tipo de facturación en la cual se factura desde el CEDI Central ubicado en carretera Masaya, se aplica con los canales de venta de oficina y tele ventas

Ventas a supermercados Wall-mart: En el tipo de venta, está dirigido a los clientes asociados a la cadena de supermercados Wal-Mart como los PALI, MAXI PALI, los cuales tienen sus políticas de descuentos especiales, este aplica al canal

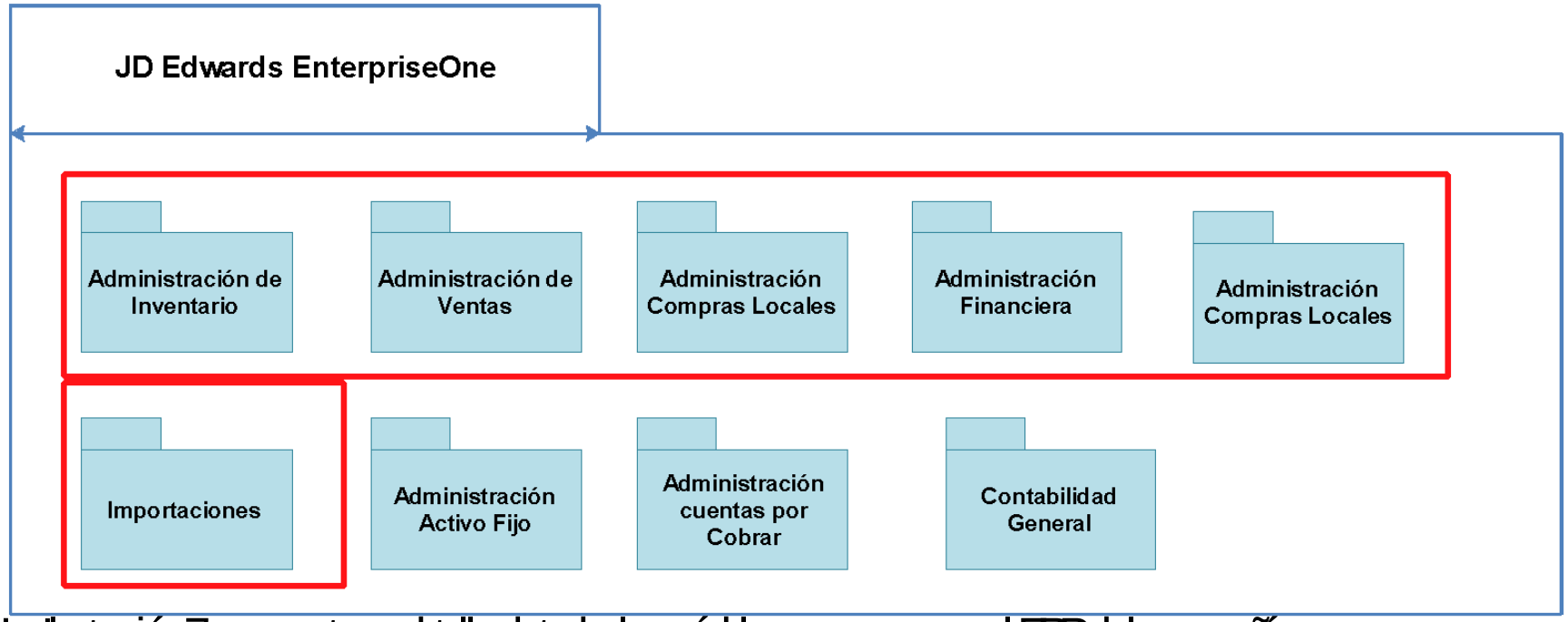
autoservicio, el modelo de venta es aplicado acá, pero se separa ya que aquí interviene el servicio de Almamater para recibir los pedidos.

9.2 SISTEMAS DE INFORMACIÓN DE LA EMPRESA OCALSA

9.2.1 JD Edwards EnterpriseOne (JDE)

De Oracle, ERP principal de la empresa, es una suite de software de planificación de recursos empresariales vigente en Ocal desde el año 2007 y que contiene los siguientes módulos:

Ilustración 7 Módulos de JDE



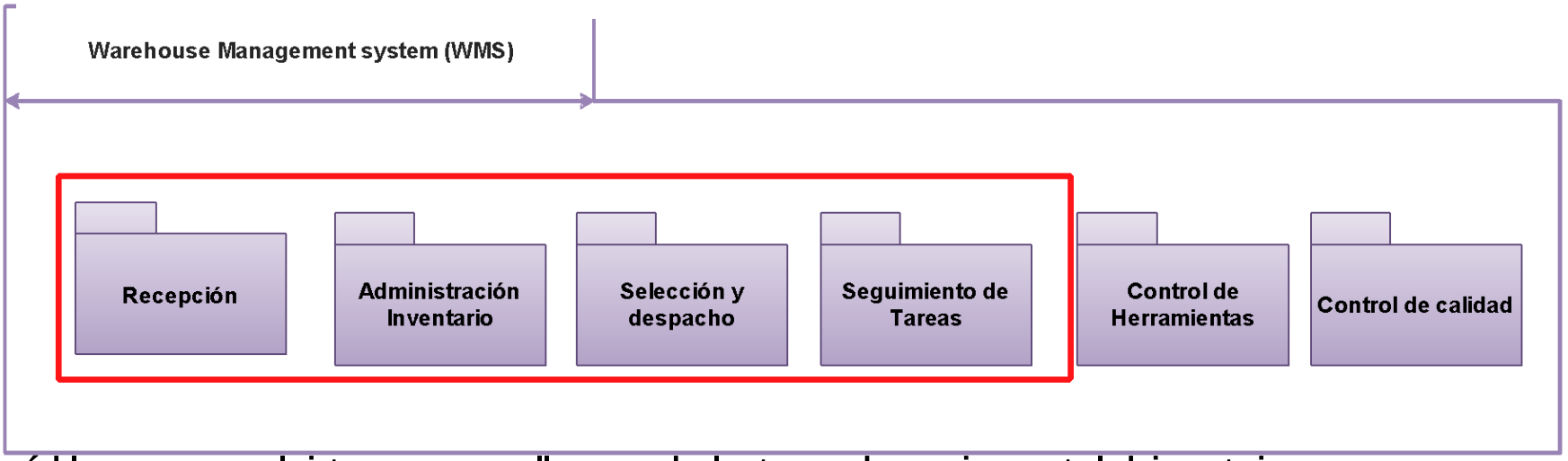
La Ilustración 7 representa un detalle de todos los módulos que operan en el ERP de la compañía

Es una suite de software de planificación de recursos empresariales completo con aplicaciones integradas que combina valor empresarial, tecnología basada en estándares y profunda experiencia del sector en una solución de negocio con un bajo coste total de propiedad. (ISOS.f.)

9.2.2 Warehouse Management System (WMS),

Es el sistema encargado de las operaciones de bodega estén automatizadas y controladas. La ilustración 8 muestra los

Ilustración 8: Estructura de WMS



módulos que posee el sistema wms para llegar a cabo las tareas de manejo y control de inventario.

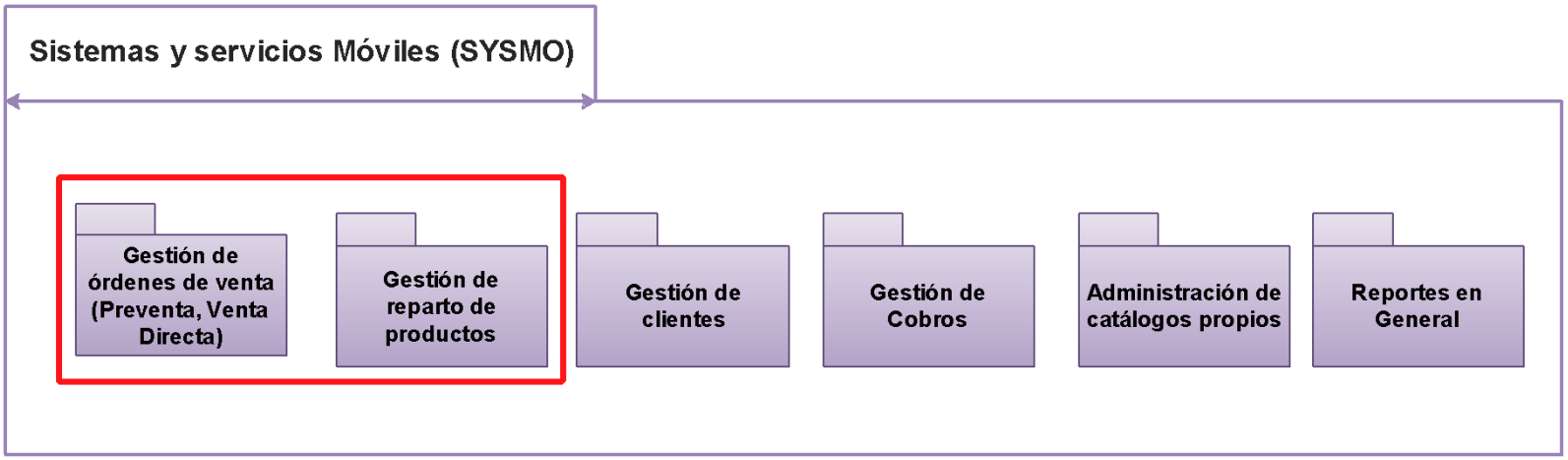
Características de EWMS

- Automatización de las bodegas
- Plataforma Web
- Móvil – Hand Held
- Back office – Administración
- Se utiliza en el CEDI-CENTRAL y CEDI-NORTE

9.2.3 Sistemas y servicios Móviles (SYSMO)

Sistema que sirve como plataforma de ventas y administración de entrega. El SYSMO incluye los siguientes procesos:

Ilustración 9 Módulos de Sysmo



La ilustración 9 representa los módulos y servicios que posee el sistema Sysmo

Sysmo Móvil: Es el sistema instalado en los equipos móviles bajo Android de los ejecutivo de ventas que operan con este tipo de facturación, y se enlaza con el sistema Back Office SYSMO, en este sistema los ejecutivos ingresan sus facturas.

Backoffice SYSMO: Es la plataforma que se encarga de manejar lo concerniente con los dispositivos móviles, además de servir de enlace con el ERP de la compañía, este recibe información de los sistemas SYSMO Móvil, POS. Adicionalmente recibe la información del ERP principal de la compañía de precios, bonificaciones, clientes, artículos todo lo necesario para que los ejecutivos de ventas pueden facturar y este lo procesa para enviarlos a los sistemas POS y SYSMO móvil.

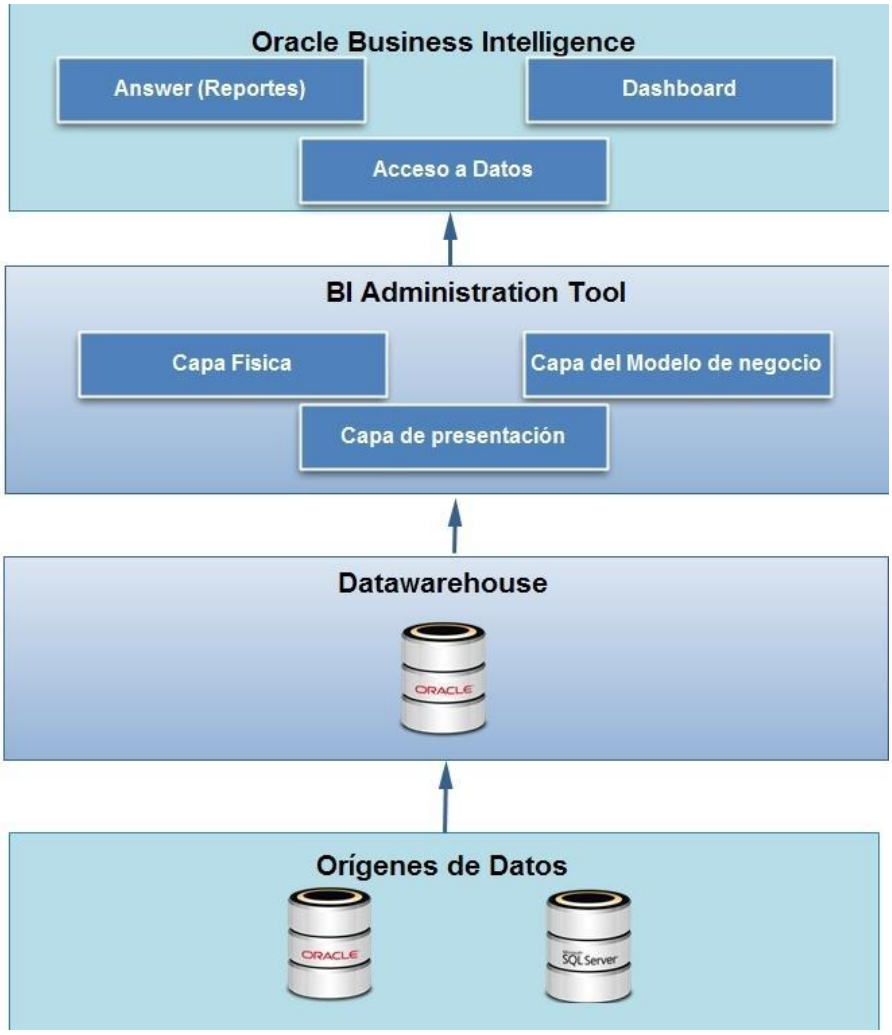
9.2.4 Sistema POS

Es el sistema instalado en los equipos de cómputo bajo Windows de la tienda zona libre, y se enlaza con el sistema Backoffice SYSMO, en este sistema los ejecutivos ingresan sus facturas.

9.2.5 Oracle Business Intelligence.

Según la empresa ORACLE en la definición de su producto tenemos que "Oracle Database 11g es una plataforma integral de base de datos para data warehousing e inteligencia de negocios que combina escalabilidad y desempeño líderes del sector, análisis bien integrado y calidad de datos e integridad— todo en una sola plataforma que se ejecuta en una infraestructura grid de bajo costo y confiable.

Ilustración 10 Estructura de Oracle Bussines Intelligence

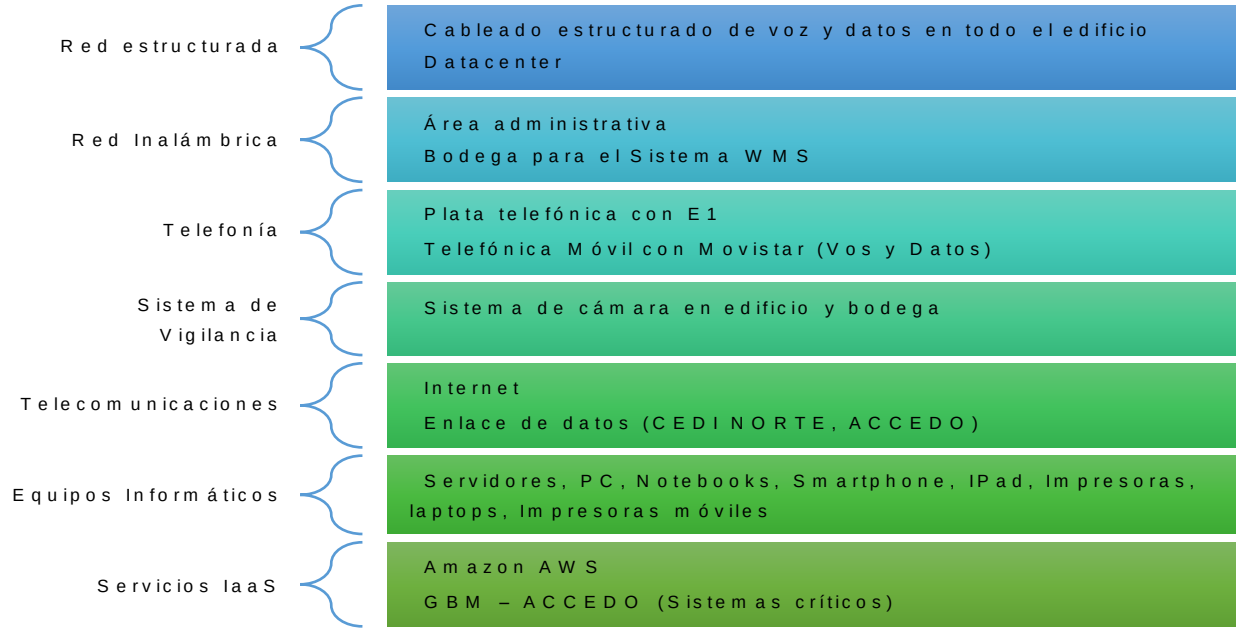


La ilustración 10 representa la estructura completa de la herramienta de Inteligencia de Negocios de Oracle, la interfaz de usuario, las herramientas de administración, el almacén de datos y los orígenes de datos.

9.3 INFRAESTRUCTURA TECNOLÓGICA DE LA COMPAÑIA

Ilustración 11 Infraestructura tecnología de la compañía OCAL SA

Ilustración 11 Infraestructura tecnología de la compañía OCAL SA

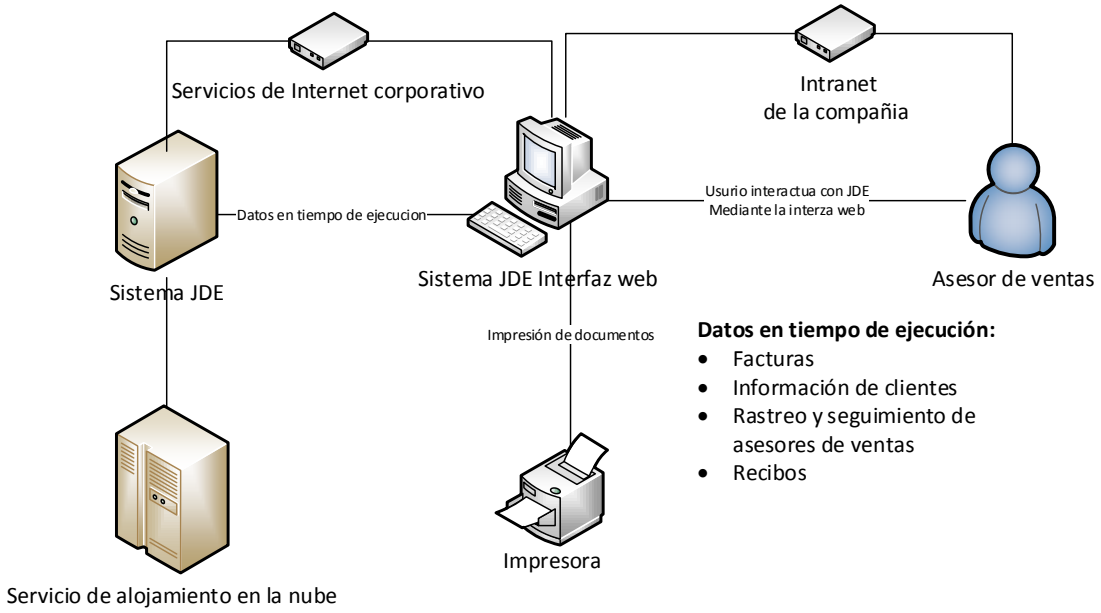


La ilustración 11 representa la infraestructura general presente en la compañía.

9.3.1 Relación de las tecnologías de la información con los usuarios y la gestión de ventas

Sistema JD Edwards y tecnologías de la información con los usuarios

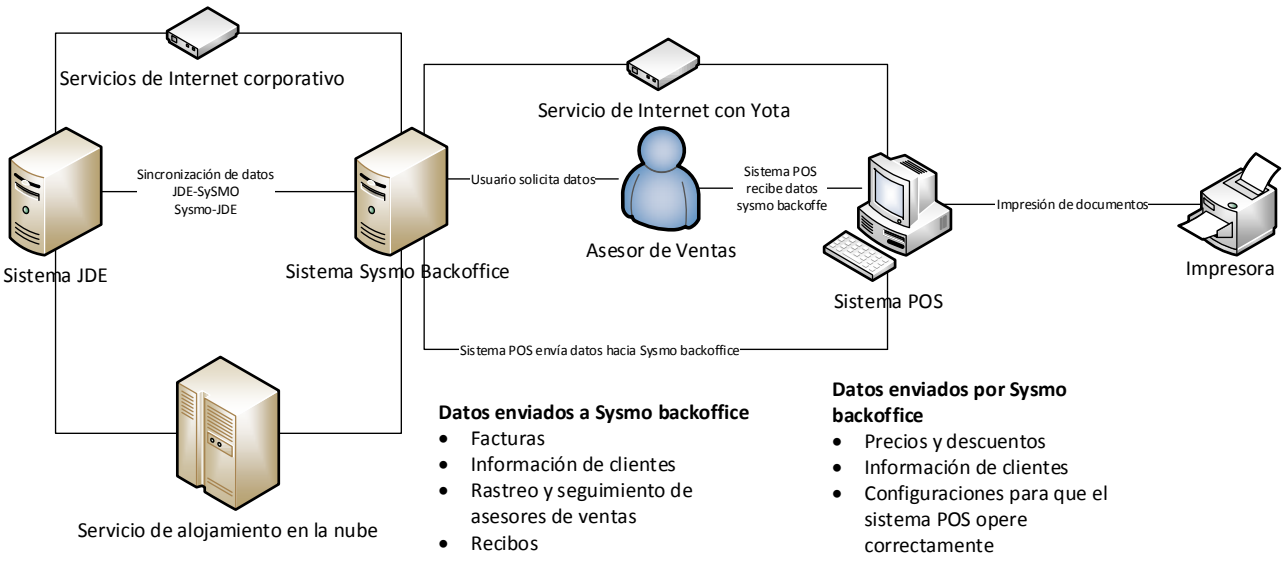
Ilustración 12 Relación JDE y tecnologías de la información -Usuarios



La **ilustración 12** representa la relación del sistema JD Edward con los usuarios finales en este caso los asesores de ventas, así como también la interacción de las tecnologías de la información con el sistema JD Edward para poder llevar a cabo las tareas de facturación este esquema se aplica en el caso del canal de venta de oficina y tele ventas.

Sistema POS y tecnologías de la información con los usuarios

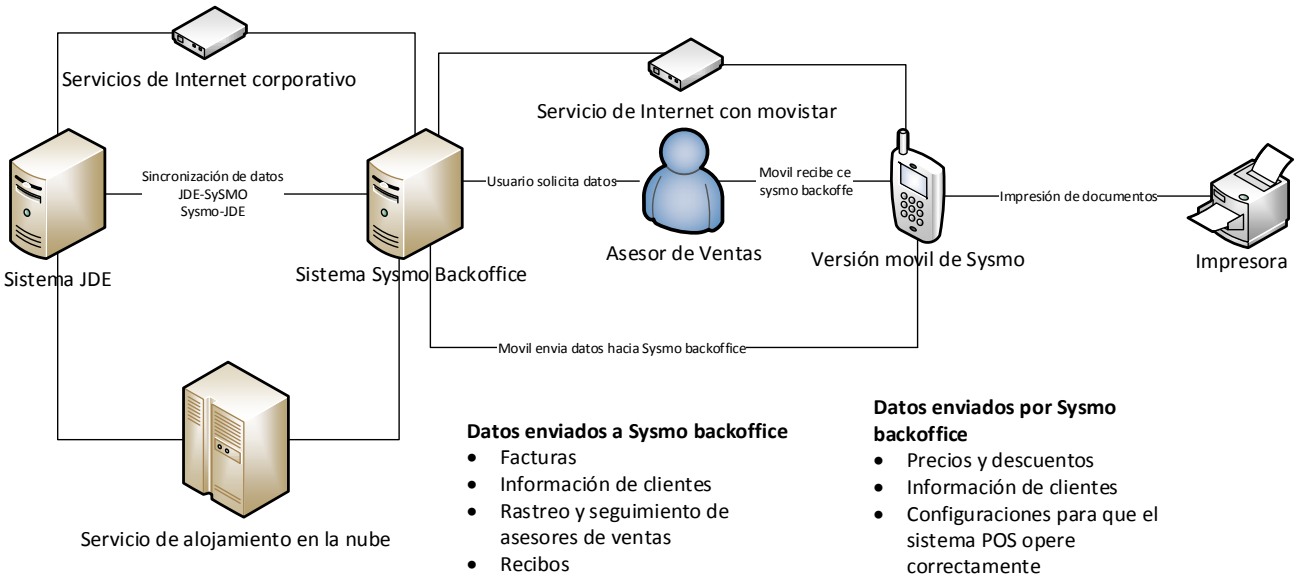
Ilustración 13 Relación POS y tecnologías de la información – Usuarios



La Ilustración 13 representa la relación del sistema POS con los usuarios finales en este caso los asesores de ventas, así como también la interacción de las tecnologías de la información con el sistema POS para poder llevar a cabo las tareas de facturación este esquema se aplica en el caso del canal de venta de tienda zona libre.

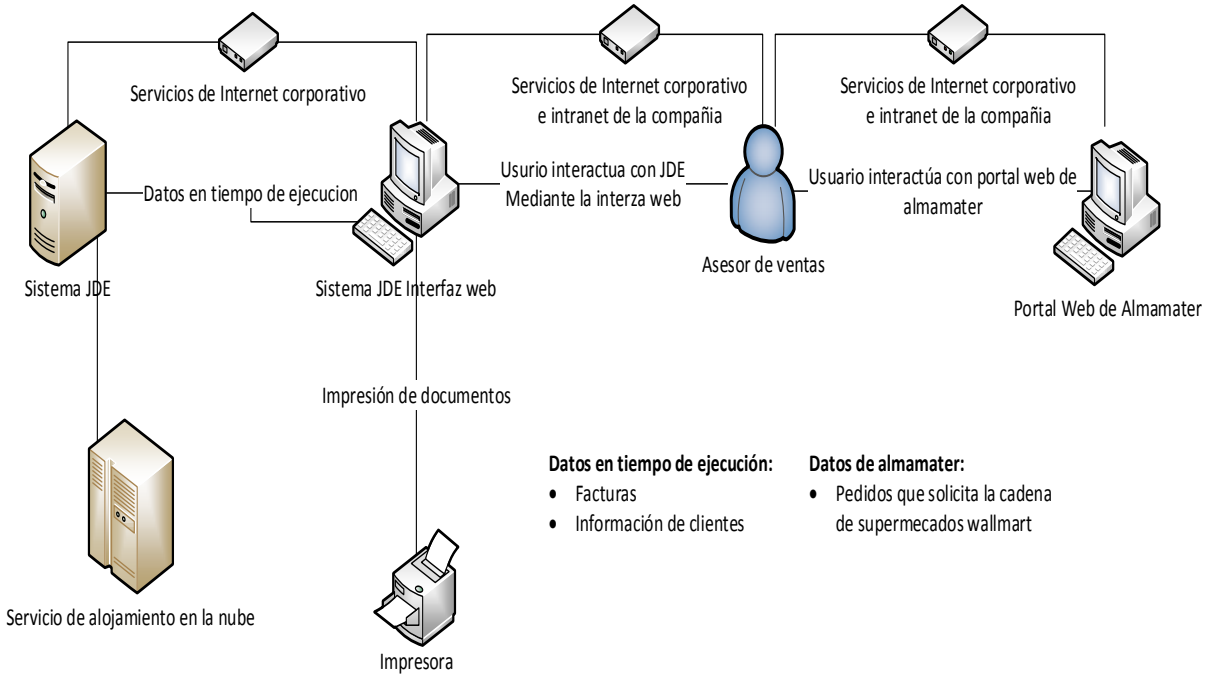
Sistema SYSMO móvil y tecnologías de la información con los usuarios

Ilustración 14 Relación SYSMO y tecnologías de la información - Usuarios



La Ilustración 14 representa la relación del sistema SYSMO móvil con los usuarios finales en este caso los asesores de ventas, así como también la interacción de las tecnologías de la información con el sistema SYSMO móvil para poder llevar a cabo las tareas de facturación este esquema se aplica en el caso a los canales de venta de Mayoreo, detalle, food services, canal perecederos.

Ilustración 15 Interacción sistema almamater, jde y usuario

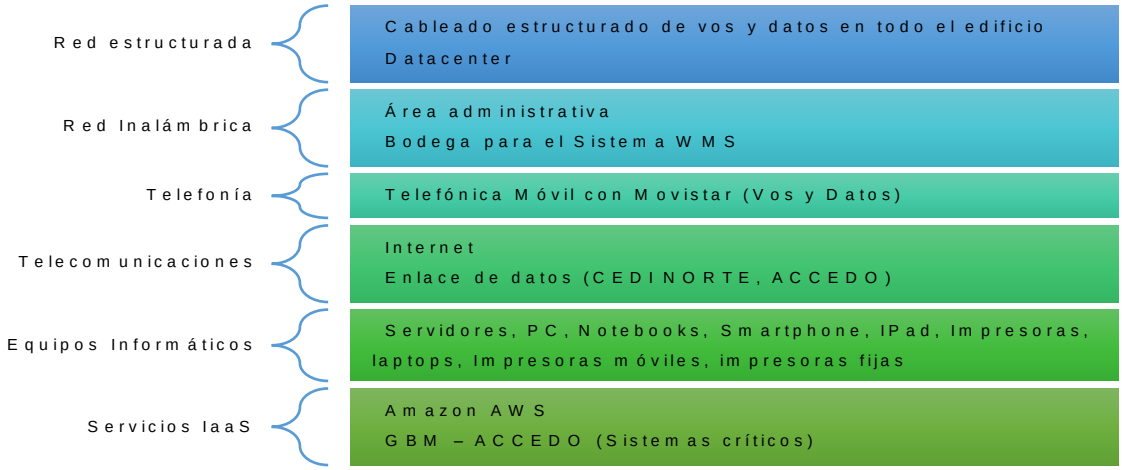


La Ilustración 15 representa la relación del sistema de almamater con los usuarios finales en este caso los asesores de ventas, así como también la interacción de las tecnologías de la información con el sistema JD Edwards para poder llevar a cabo las tareas de facturación en este caso se aplica para la facturación con los supermercados de la cadena walmart.

9.3.2 Infraestructura tecnología en la gestión de ventas

Estructura Tecnológica asociada a la modalidad de venta directa

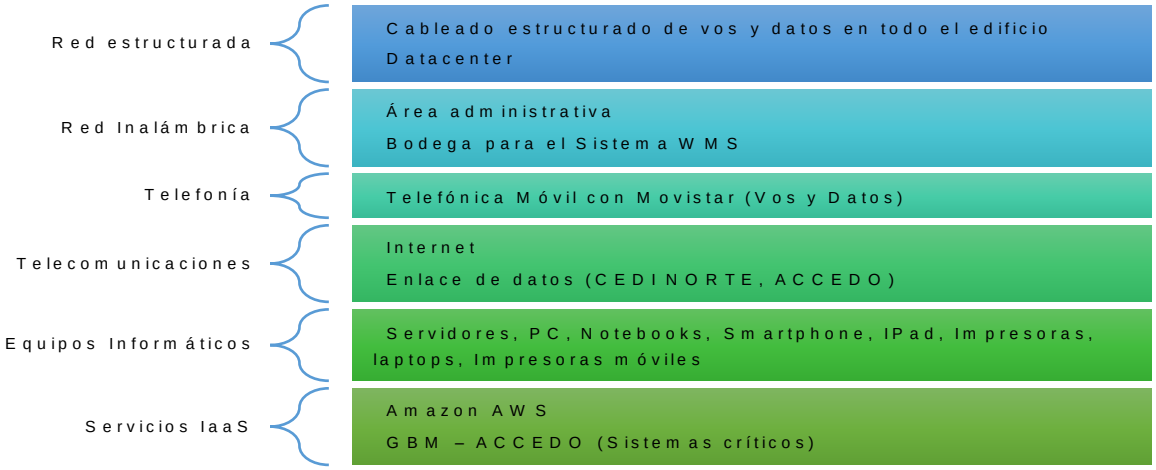
Ilustración 16 Tecnologías informáticas involucradas en la modalidad de venta directa



La Ilustración 16 detalla las tecnologías informáticas involucradas en el modo de venta directa.

Estructura Tecnológica asociada a la modalidad de preventa

Ilustración 17 Tecnología de la información asociada a la modalidad de preventa

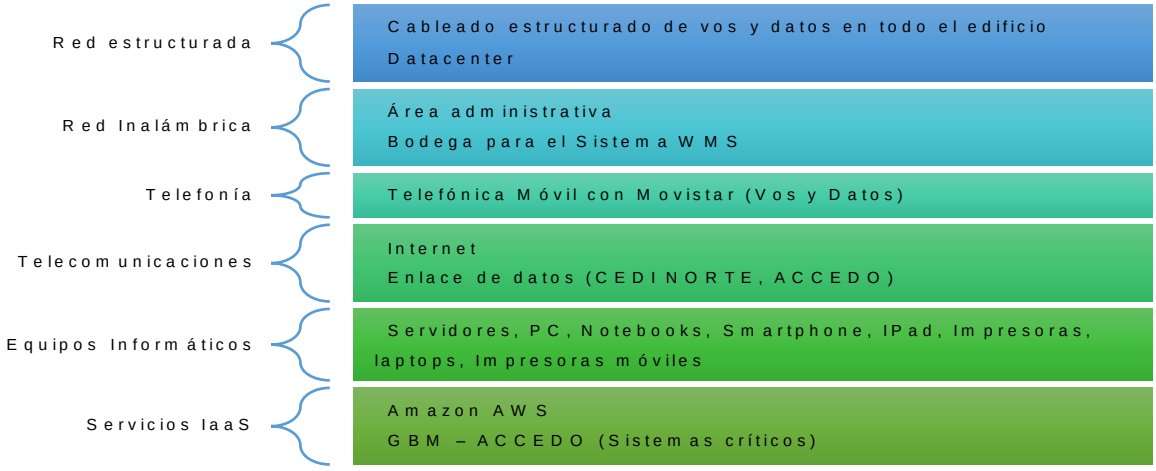


La Ilustración 17 detalla las tecnologías informáticas involucradas en la modalidad de facturación de preventa.

Ventas de oficina: Este tipo de facturación en la cual se factura desde el CEDI Central ubicado en carretera Masaya.

Estructura Tecnológica asociada a la modalidad de oficina

Ilustración 18 Tecnologías de la información en la modalidad venta de oficina

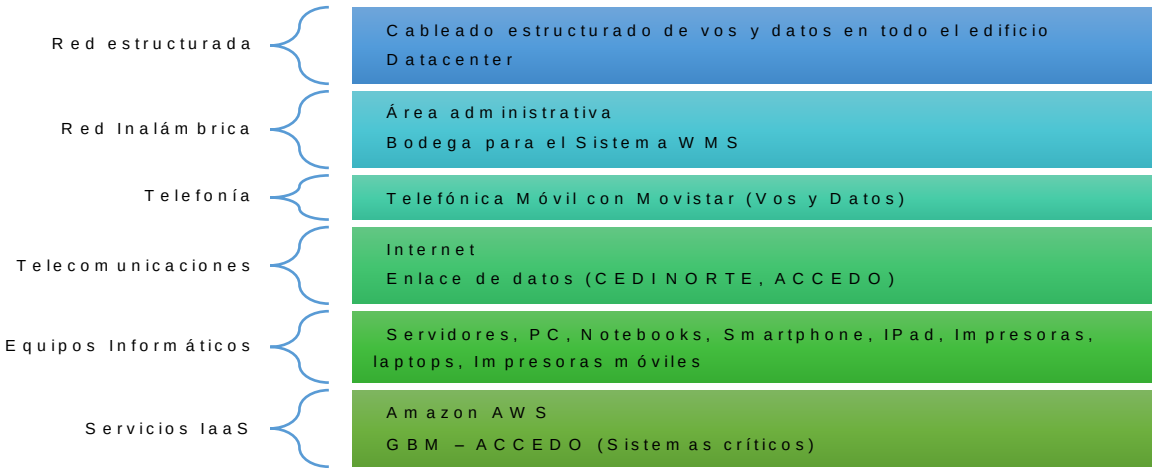


La Ilustración 18 detalla las tecnologías informáticas involucradas en la modalidad de facturación de venta de oficina.

Ventas a supermercados Walmart

Estructura Tecnológica asociada a la modalidad dirigida a Walmart

Ilustración 19 Estructura tecnología informática a la modalidad dirigida a wallmart



La Ilustración 19 representa las tecnologías informáticas presentes en el proceso de venta en la modalidad de supermercados walmart

9.4 DESARROLLO DE ANALISIS DE RIESGOS

La conducción del Caso de estudio se apega a las consideraciones generales de la empresa.

Por razones de confidencialidad, se debe de omitir información concerniente con información de precios, promociones, información de los clientes.

De acuerdo con las características descritas en el diseño del Estudio, se realizó la correspondencia:

Gerente de Tecnología

- Gerente de Tecnología y comunicaciones

Jefes de Área

- Jefe de Departamento de Soporte Técnico
- Jefe de Departamento de Desarrollo e Integración de Sistemas

Técnicos de Área

- Analista de Sistemas
- Técnico de Soporte Técnico

Ejecutivos de Ventas

- Vendedores de Perecederos
- Vendedores de Ventas de Oficina
- Vendedores de Canal Mayorista
- Vendedores de Canal Autoservicio
- Vendedores de Canal Food Service

El primer bloque de entrevistas está dirigido al Gerente de Tecnología y comunicaciones, al Jefe de Soporte Técnico y el departamento de desarrollo e integración de sistema de la empresa, con el objetivo de identificar los objetivos de la compañía, así como el compromiso de la gerencia de tecnología y comunicaciones con la compañía, para estos se utilizó un cuestionario con preguntas abiertas (ver Anexo 3) A continuación, una síntesis de las entrevistas:

Las operaciones de facturación de la compañía deben de poder efectuarse sin interrupciones, por ende, el compromiso de la gerencia de TIC, es garantizar que las tecnologías de la información que soportan dichas operaciones funcionen de manera óptima para que la empresa pueda cumplir las metas de ventas propuestas.

A continuación de esta reunión se presenta un listado de riesgos que fueron mencionados por los participantes:

- Corrupción/Falla de Software de Maquina Virtuales
- Corrupción de Base de Datos SQL Server
- Corrupción de Base de Datos Oracle
- Corrupción de Base de Respaldos Datos SQL Server
- Corrupción de Base de Respaldos Datos Oracle
- Falta/Falla de Respaldos de los sistemas principales
- Falta/Falla de Respaldos de Máquinas Virtuales
- Falta/Falla de Respaldos de Bases de Datos
- Falla de Paquete de Servicios de Internet Corporativo
- Falla con Servicios de Proveedor de Almacenamiento en la Nube
- Manejo inadecuado de datos críticos (codificar, borrar)
- Unidades portables con información sin cifrado
- Transmisión no cifrada de datos críticos
- Manejo inadecuado de contraseñas
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por medios no oficiales
- Violación a derechos de autor
- Ataque informático
- Robo (físico) Smartphone
- Robo (físico) Computadora laptop
- Robo (físico) Computadora Tablet
- Robo (físico) Computadora PC
- Robo (físico) PDA
- Espacio de almacenamiento insuficiente
- Falla en la plataforma de almamater

En el segundo bloque de entrevistas, se dirigió a los técnicos de soporte técnico y a los analistas de sistemas de la compañía los cuales se encuentran en el CEDI

Central los cuales, debido a sus funciones dentro de la compañía descritos anteriormente, la entrevista se enfocó en los incidentes que se presentan en la compañía, para dichas entrevistas se ocupó el cuestionario con preguntas cerradas abiertas (ver Anexo 2) A continuación, se presenta un listado de riesgos que han mencionado los técnicos de soporte técnico y los analistas de sistemas de sistemas:

- Ataque físico a los equipos informáticos
- Ataque informático
- Daños por vandalismo
- Fraude (Estafa)
- Robo (físico) Computadoras
- Robo (Físico) Smartphone
- Robo (Físico) PDA
- Robo (Fisco) Tablet
- Robo (Físico) Laptop
- Virus
- Sismos
- Polvo
- Falla Fluido eléctrico
- Malmanejo de sistemas y herramientas
- Utilizar programas no autorizado
- Unidades portables sin cifrado
- Manejo inadecuado de contraseñas (inseguras, no cambiar)
- Compartir contraseñas o permisos a terceros no autorizados
- Exposición o extravío de equipo, unidades de almacenamiento
- Acceso no autorizado
- Falla de sistema principal
- Falla en Herramientas de MS Office
- Falla/Daño en los smartphones
- Falla/Daño en Impresoras Móviles

- Falla/Daño en Impresoras Fijas
- Falla/Daño en Físico Tablets
- Falla/Daño en Físico en PDA
- Falla/Daño Físico en Computadora
- Falla en la Infraestructura interna de Red
- Falla de Paquete de Servicios de Internet Móvil
- Falla de Paquete de Servicios de Internet Corporativo
- Falla con Servicios de Proveedor de Almacenamiento en la Nube
- Falta de definición de perfil, privilegios y restricciones del personal
- Falta de mantenimiento físico (repuestos e insumos)
- Falta de actualización de software
- Acceso no autorizado a sistemas externos
- Acceso no autorizado a sistemas internos
- Red cableada expuesta para el acceso no autorizado
- Red inalámbrica expuesta al acceso no autorizado
- Dependencia a servicio técnico externo

El tercer bloque de entrevistas está dirigido a los usuarios finales de los sistemas de información y la infraestructura tecnología de la compañía, en este caso como el Caso de estudio descrito está enfocado en los procesos de facturación de la compañía, el perfil que se necesita es de los ejecutivos de ventas de los distintos canales de la compañía, estos se han divido según la modalidad de ventas que trabajan los canales, para esto se utilizó un cuestionario con preguntas cerradas (Anexo 1) las cuales fueron diseñadas específicamente para los ejecutivos de ventas :

En el proceso de venta directa se utilizó el cuestionario 2 y participaron 2 personas como resultado de las entrevistas se determinaron los siguientes riesgos

- Falla en sistemas de facturación

- Falla en los servicios de internet
- Fallo en sistema POS (Sistema del banco)
- Carga en batería de celular (se agota rápidamente)

En la modalidad de preventa se utilizó el cuestionario 3 y participaron 14 personas como resultado de las entrevistas se determinaron los siguientes riesgos.

- Carga en batería de celular (se agota rápidamente)
- Falla en sistemas de facturación
- Falla en los servicios de internet

En modalidad de venta de oficina se utilizó el cuestionario 2 y participaron 2 personas como resultado de las entrevistas se determinaron los siguientes riesgos

- Daño en batería (respaldo ups)
- Fallo en equipo de computadora

En la modalidad de venta de supermercados walmart se utilizó el cuestionario 2 y participaron 2 personas como resultado de las entrevistas se determinaron los siguientes riesgos

- Falla en sistemas de facturación
- Daño en batería (respaldo ups)
- Fallo en equipo de computadora

Para la valoración de riesgo se consolida en una sola lista los riesgos declarados de las síntesis anteriores, como se presenta a continuación:

1. Falla en sistemas de facturación **Causa u origen** se originan debido a configuraciones realizadas por parte de los usuarios administrativos, que ocasionan que los ejecutivos de venta no puedan usar los sistemas para las tareas que ellos necesitan o inclusive errores en la creación de facturación a los clientes, estas fallas pueden ser errores de precio, errores de censo y/o errores de productos, esto afecta a los sistemas SYSMO, POS OCAL, JD Edwards. **Consecuencias**: Retrasos en las tareas de facturación de los ejecutivos de ventas, esto puede afectar a cualquier ejecutivo en cualquier canal, por lo general afecta a máximo 3 ejecutivos de ventas **Frecuencia de ocurrencia:** Se presenta almenos 2 veces al mes, su duración es de 15 minutos y ocurre por lo común al inicio de la jornada laboral. **Costo**. El evento cuesta 295 $ por media hora que se presenta el evento al mes

2. Daño en batería (respaldo ups). **Causa u origen** Son fallos en los respaldos de batería para los equipos de escritorio esto ocasiona que cuando se presente un inconveniente con el fluido eléctrico el equipo se apague y posiblemente se pierda la información que todavía no está guardada. **Consecuencias:** perdidas de información de los usuarios, Daños en los componentes físicos o corrupción del sistema operativo instalado en el equipo, Impedimento de las operaciones de los usuarios la afectación se da a los usuarios del canal tele ventas. **Frecuencia de ocurrencia:** Este evento se da por tiempo de uso de los ups puede durar su vida útil 2 años, el evento puede afectar a 1 ejecutivo media hora **Costo:** el costo de la batería puede rondar los 60 $, el costo en venta 72 $, el total seria 132 $

3. Fallo en equipo de computadora en oficina **Causa u origen:** Falla en los componentes físicos de los equipos de escritorio y/o sistema operativo. **Consecuencias:** perdidas de información de los usuarios instaladas, Impedimento de las operaciones de los usuarios de facturación que usan el equipo, esto afecta al canal tele ventas, afectado las operaciones de facturación del ejecutivo **Frecuencia de ocurrencia:** Este evento se da por tiempo de uso de los equipos este evento se

puede producir 1 vez cada año, el evento dura 2 horas **Costo** el costo del evento se promedia 394 $ por hora, costo relacionado con el costo del equipo 400 $ si este no se puede recuperar, en todo caso si se da esto último se reemplaza el equipo, este afecta a 1 ejecutivo, en total 794$

4. Falla en los servicios de internet **Causa u origen** esto ser refiere a los servicios de internet con proveedores comerciales (YOTA, CLARO, MOVISTAR) que forman parte de la integración con los sistemas que funcionan fuera de la compañía (como SYSMO móvil, y el sistema POS de OCAL). **Consecuencias:** problemas con recibir información actualizada en los sistemas y enviar la información para ser procesadas en el CEDI Central o Cedi Norte, Retrasos en las operaciones de facturación, esto puede afectar a todos procesos de facturación de preventa y venta directa. **Frecuencia de ocurrencia:** Esto dependerá del lugar donde esté ubicado el ejecutivo de ventas, se deja por fuera el factor en el cual el plan de datos ha sido agotado o el pago del servicio no ha sido efectuado, solo es tomado el factor cuando el servicio falla por problema con el proveedor del servicio este evento se puede presentar cada 1 vez en periodo de 6 meses, la duración del evento puede llegar a durar 2 horas y afecta por lo común a 20 ejecutivos máximo. **Costo** tomando en cuenta que esto afecta a varios el costo puede ser 7880 $

5. Fallo en sistema POS (Sistema del banco) **Causa u origen** mal funcionamiento del equipo POS proporciono por el banco. **Consecuencias** impedimento de facilitar pagos para los clientes, Impedir que los clientes realicen pagos con tarjeta de crédito, Perdida de venta por no tener disponible este medio, Insatisfacción de los clientes, esto se ha reportado nada más en los modelos de venta de oficina y venta directa **Frecuencia de ocurrencia:** Este evento no es muy frecuente, se ha reportado un incidente cada 9 meses, en incidentes aislados, y puede durar 4 horas, lo presenta solo 1 ejecutivo, El costo puede ser de 788 $.

6. Carga en batería de celular (se agota rápidamente) **Causa u origen** la batería de los equipos móviles de los ejecutivos de ventas se agota más rápido de lo normal, esto por el uso constante del móvil en las tareas de los ejecutivos de ventas, esto se presenta en el modelo de preventa y venta directa(canal perecedero) **Consecuencias** Paralización y/o retraso de las operaciones de los ejecutivos de ventas **Frecuencia de ocurrencia:** todos los días, pero se puede reducir ya que los ejecutivos cargan una batería recargable. El costo se asocia al precio de cargador 70 $.

7. Ataque físico **Causa u origen** esto se refiere al daño provocado por acciones de los usuarios tales como caídas, golpes a los equipos informáticos (Smartphones, tablets, computadora de escritorio, laptop). **Consecuencias:** Costos asociados con el reemplazo o con el uso de servicios para reparar los daños. **Frecuencia de ocurrencia:** no es frecuente intencionalmente, esto se puede presentar en cualquier modelo de venta, y suele sucederle a 1 solo ejecutivo de ventas. El costo será asociado directamente al costo del equipo dañado entre 300 $ y 900 $

8. Ataque informático **Causa u origen** acciones provocadas por ataques informáticos a los servicios informáticos, base de datos, aplicaciones web. Perdida de información crítica, costos asociados con la reparación de los servicios informáticos, inconvenientes con las operaciones de la compañía. **Consecuencias:** Perdida de información crítica, Costos asociados con la reparación de los servicios informáticos. Inconvenientes con las operaciones de facturación de la compañía, paralización de las operaciones dela compañía, afectación a todos procesos de facturación de la compañía. **Frecuencia de ocurrencia:** Todos los días. **Costo**: El costo asociado está dirigido al costo de mantenimiento de licencias de software de seguridad, este puede llegar a ser de 10,000 dólares anuales.

9. Daños por vandalismo **Causa o fuente** esto se refiere al daño provocado por actividades delictivas, a los equipos o infraestructura tecnológica de la compañía

Consecuencias: Costos asociados con el reemplazo o el uso de servicios externos para reparar los daños. **Frecuencia de ocurrencia:** no se ha producido ningún incidente desde hace 10 años.

10. Fraude (Estafa) **Causa u origen** daños monetarios provocados por fraudes provocados, ya sea por los usuarios a la empresa o estafas hechas hacia los ejecutivos de ventas, utilizando vulnerabilidades en los sistemas de información. **Consecuencias:** Perjuicios a la imagen de la compañía con los clientes, Daños económicos. **Frecuencia de ocurrencia:** Este tipo de eventos se ha presentado 2 veces en los últimos 7 años. **Costo** el costo ha sido alrededor de los 1000 $.

11. Robo (físico) **Causa u origen** Computadoras PC este riesgo se refiere al hurto de equipos de computador de oficina. Consecuencias costos asociados con el reemplazo de los equipos y retraso de las actividades de los ejecutivos de ventas, esto afecta el proceso de venta de oficina **Consecuencias:** Costos relacionados con los equipos de cómputo, Retraso en las operaciones del ejecutivo el cual tiene asignado el equipo. **Frecuencia de ocurrencia:** Tiene más de 10 años sin pasar. **Costo** el costo del de un equipo de pc es 400 $

12. Ataque de virus informático **Causa u origen** este refiere al hecho que el sistema operativo de las computadoras, Smartphone, Tablet sea infectado con un virus que afecte sus funcionalidades. **Consecuencias** paralización y/o retraso de las operaciones del ejecutivo de ventas, daños en los equipos de cómputo, Retraso en las operaciones del ejecutivo de ventas, Perdida de información del equipo afectado**,** Costos relacionados con el equipo de cómputo, este puede afectar a cualquier canal de ventas, puede afectar a toda la empresa en el caso más grave. **Frecuencia de ocurrencia:** todos los días. **Costo** El costo asociado está dirigido al costo de mantenimiento de licencias de software de seguridad, este puede llegar a ser de 10,000 dólares anuales

13. Sismos **Causa u origen** los sismos son un riesgo natural que afecta a la compañía y comprometer las operaciones de la compañía. **Consecuencias** afectación en las operaciones de la compañía, Paralización de las operaciones de facturación de la compañía. **Frecuencia de ocurrencia:** Esto es un evento natural, el cual no puede ser controlado ni pronosticado y está en todo momento, por lo tanto, es todos los días. **Costo** El costo puede llegar a interrumpir las operaciones del día, llegarlas a cortar a la mitad del día por lo tanto el costo es de 57,708.92 de dólares.

14. Polvo **Causa u origen** el polvo afecta los componentes electrónicos de los equipos de cómputo, Smartphone de la compañía. **Consecuencias**: Deterioro en los equipos electrónicos de la compañía, Costo relacionado con la reparación. **Frecuencia de ocurrencia:** Todos los días. **Costo** el mantenimiento de los equipos se da en la propia empresa, 1 vez cada seis meses, el gasto se da en los componentes que usan para dar mantenimiento a los equipos, este puede rondar por los 60 $.

15. Falla Fluido eléctrico **Causa u origen** se refiere a las fallas en el servicio de energía eléctrica de la compañía. **Consecuencias:** Paralización de las operaciones internas de la compañía, Paralización de las operaciones de facturación de la compañía. **Frecuencia de ocurrencia:** Por lo menos 3 o 4 días a la semana. El costo está asociado con el costo del combustible que ocupa la planta 600 $

16. Mal manejo de sistemas y herramientas informáticas **Causa u origen** Esto se refiere al uso inadecuado de los sistemas o lo equipos informáticos de la compañía, provocando inconsistencias en la información y provocando inconvenientes en las operaciones de facturación de la empresa o inconformidad con los clientes, esto es más frecuenta en el canal detalle y autor servicio. **Consecuencias:** Insatisfacción de los clientes al no recibir sus productos, no cerrar tratos comerciales con los clientes, retrasos en las operaciones de facturación, esto puede afectar a cualquiera de los procesos de facturación **Frecuencia de ocurrencia:** este incidente solo se presenta

al tener nuevo personal en la compañía y aun así no es muy frecuente, puede presentarse 4 veces en un periodo de 10 meses, este evento puede 30 minutos en lo que se brinda el soporte necesario, 1 ejecutivo se afecta. **Costo** el promedio del costo que puede costar es 98.2 $.

17. Utilizar programas no autorizado **Causa o fuente** Cuando los usuarios instalan programas no autorizados en los equipos informáticos de la empresa. **Consecuencias:** Problemas con derechos de autor, posibles demandas que incurren en una indemnización monetaria, si el software es licenciado, Ataques informáticos derivados del uso de software no autorizado por la gerencia de tecnología, ya que estos pueden contener código malicioso, Contagiar de virus a los equipos informáticos por el uso de software no autorizado. **Frecuencia de ocurrencia:** esto nunca se presenta ya que la gerencia de tecnología controla la instalación y restringe por reglas de dominio la instalación de software en los equipos de los procesos de facturación. **Costo** relacionado a las multas que pueda sufrir la empresa

18. Unidades portables sin cifrado **Causa u origen** El uso de dispositivos de almacenamiento externos sin cifrado, los cuales poseen información confidencial de la compañía. **Consecuencias:** Información confidencial tales como precios y/o promociones pueden caer en manos de la competencia. **Frecuencia de ocurrencia:** este evento no es muy frecuente ya que los equipos de escritorio tienen restringido el uso de dispositivos USB, el acceso a ocupar estos dispositivos está restringido por permiso, pero cuando se realiza no tienen cifrado. **Costo** este evento no produce afectación en la facturación.

19. Manejo inadecuado de contraseñas (inseguras, no cambiar) **Causa u origen** Se refiere al hecho de tener contraseñas inseguras de acceso a los sistemas principales, o no realizar el cambio de estas periódicamente. **Consecuencias:** Información confidencial tales como precios y/o promociones pueden caer en manos

ajenas a la compañía. **Frecuencia de ocurrencia:** Esto sucede muy frecuentemente 2 veces al mes. **Costo** este evento no produce afectación en la facturación.

20. Transmisión de contraseñas por medios no oficiales **Causa u origen** Los usuarios transmiten contraseñas entre si vía chat de whatsapp o mensajería de texto de celular. **Consecuencias:** Al tratarse de medio no oficiales, alguien puede acceder ajeno a la compañía puede acceder a información de la compañía. **Frecuencia de ocurrencia:** Esto sucede muy frecuente por lo menos 2 veces al mes. **Costo** este evento no produce afectación en la facturación

21. Compartir contraseñas o permisos a terceros no autorizados **Causa u origen** Esto es debido al mal concepto que los usuarios poseen del uso de contraseñas y la seguridad, ya que algunos usuarios tienen acceso a información a la cual según su jerarquía no debería de tener, la razón por la que el personal presta su contraseña para realizar labores a los cuales ellos no quieren prestar la atención debida. **Consecuencias:** Personal externo puede acceder a información de la compañía, Personal interno de la compañía tendría acceso a información la cual no es apta para su nivel jerárquico en la empresa. **Frecuencia de ocurrencia:** Esto es muy frecuente entre los usuarios por lo menos 4 veces al mes. **Costo** este evento no produce afectación en la facturación

22. Exposición o extravío de equipo, unidades de almacenamiento **Causa u origen** Esto es cuando los usuarios pierden los equipos informáticos o dispositivos de almacenamiento asignados por descuidos. **Consecuencias:** Costos asociados al reemplazo de los equipos perdidos, Perdida de información almacenada en los equipos**. Frecuencia de ocurrencia:** El evento se podría presentar 1 veces entre 7 meses, **Costo** este evento no produce afectación en la facturación.

23. Falla de sistema principal **Causa o fuente** Estos son incidentes relacionados cuando se dan incidentes y/o fallas del tipo técnicas (solamente en la cual tienen injerencia los técnicos de sistemas y/o soporte técnico) en el ERP principal de la

compañía JD Edwards **Consecuencias:** Paralización total de las operaciones de la compañía, paralización de las operaciones de facturación, la afectación se da en todos los procesos de facturación. **Frecuencia de ocurrencia:** El evento se presenta una vez al año, y su duración abarca 1 horas **Costo** este evento puede incurrir en un monto de venta igual 14,427 $

24. Falla en Herramientas de MS Office **Causa u origen** Esto es cuando el software de Microsoft office presenta inconvenientes e impiden trabajar en estas herramientas.

Consecuencias: Retraso en las operaciones que realizan los asesores y/o supervisores que dependan de estas herramientas, las cuales no afectan las operaciones de ventas**. Frecuencia de ocurrencia:** El evento no es muy frecuente, 2 veces al entre 4 meses. **Costo** no tiene efecto sobre la venta

25. Falla/Daño en los smartphones **Causa u origen** Fallos, daños provocadores por los usuarios a los smarphones o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados al valor de los equipos que se deben de reemplazar, Retrasos en las operaciones de facturación del ejecutivo de ventas, esto puede afectar por lo común a los procesos de venta directa y preventa, por lo general solo afecta a 1 ejecutivo, pero este puede afectar toda la jornada laboral. **Frecuencia de ocurrencia:** la frecuencia está en dependencia del desgaste de los equipos, estos se cambian cada año por ende un fallo de estos puede presentarse 1 vez cada 11 meses, con un periodo de duración de 8 horas. **Costo** de los equipos se valora 290 $, el costo puede llegar a 1576 $ el total es 1866 $.

26. Falla/Daño en Impresoras Móviles **Causa u origen** Fallos, daños provocadores por los usuarios a los Impresoras o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados con el reemplazo de las impresoras móviles, en caso del cliente requiera su factura y no tener la impresora esto puede con llevar a que el cliente no quiera hacer el trato con el ejecutivo de venta o rechazar el producto

en el caso de venta directa, esto afecta al modo de facturación preventa y venta directa. **Frecuencia de ocurrencia:** El evento se produce 1 vez cada 12 meses. **Costo** el costo de una impresora son 300 $ si se reemplaza.

27. Falla/Daño en Impresoras Fijas **Causa u origen** Fallos, daños provocadores por los usuarios a los Impresoras Fijas o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados con el reemplazo de las impresoras fijas, en caso del cliente requiera su factura y no tener la impresora esto puede conllevar a que el cliente no quiera hacer el trato con el vendedor o rechazar el producto en el caso de venta directa. **Frecuencia de ocurrencia:** El evento se produce más o menos 1 vez cada 6 meses. **Costo** de una impresora ronda alrededor de 550 $,

28. Falla/Daño en Físico Tablet **Causa u origen** Fallos, daños provocadores por los usuarios a los Tablet o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados al reemplazo del equipo en este caso solo hay dos supervisores que tienen Tablet, Perdida de información del ejecutivo de ventas. **Frecuencia de ocurrencia:** la frecuencia está en dependencia del desgaste de los equipos, estos se cambian cada año por ende un fallo de estos puede presentarse 1 vez cada 3 meses. **Costo** de una Tablet es 200 $.

29. Falla/Daño en Físico en PDA **Causa u origen** Fallos, daños provocadores por los usuarios a los PDA o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados al reemplazo del equipo, el costo de las PDA ya no se toma en cuenta ya que a pesar de estar dentro del inventario de tecnología estas ya no están en uso. **Frecuencia de ocurrencia:** este evento queda descartado ya que los vendedores ya no ocupan PDA.

30. Falla/Daño Físico en Computadora táctil de la tienda zona libre **Causa o fuente** Fallos, daños provocadores por los usuarios a Computadora o por el desgaste del uso del equipo. **Consecuencias:** Costos asociados con el reemplazo

de las impresoras fijas, Retrasos en las tareas de facturación, en el caso de los ejecutivos de venta de la tienda zona libre. **Frecuencia de ocurrencia:** el evento se puede producir 1 vez en 12 meses. **Costo** el costo de un equipo ronda alrededor de 700 $. Costos asociados con el reemplazo de los equipos, el evento 16 horas, el costo de este evento 3152 $, ya que por las restricciones del aeropuerto no se puede hacer el reemplazo de los equipos en menos tiempo, el costo total es 3852 $

31. Falla en la Infraestructura interna de Red **Causa u origen** Esto se debe cuando la infraestructura de red interna (intranet) de la compañía presenta y afecta las operaciones internas de la compañía, ya sea por fallos del servidor de dominio y/o fallas provocadas por daños en la estructura cableada de la empresa, este modelo afecta al proceso s de preventa y venta de oficina. **Consecuencias:** Paralización de las operaciones de la compañía, Retrasos en las operaciones de facturación, afectación a los procesos de facturación de preventa y venta de oficina **Frecuencia de ocurrencia:** el evento se ha producido 1 vez a lo largo de 13 meses, y su duración ha sido de 10 minutos, **Costo** el evento se calcula que tiene un costo de 2328. $.

32. Falla de Paquete de Servicios de Internet Móvil (falta de pago del servicio) **Causa u origen** Falla en los servicios de internet móvil que ocupan los usuarios (ejecutivos de ventas), estos son necesarios para transmitir y recibir información para poder realizar la facturación, este puede afectar a los procesos de preventa y venta directa **Consecuencias:** Retraso en las operaciones de facturación, Los ejecutivos de ventas no reciben la información adecuada para poder cumplir con sus operaciones, No poder facturar los pedidos en tiempo y forma por la falta de envió de estos, Insatisfacción con los clientes **Frecuencia de ocurrencia:** el evento se ha producido 1 vez a lo largo de 12 meses, puede afectar 20 ejecutivos, por 15 minutos, **Costo** El costo del evento 985 $

33. Falla de Paquete de Servicios de Internet Corporativo **Causa u origen** Es cuando los servicios de los proveedores de internet corporativo, fallan en brindar este servicio y por ende los servicios de comunicación con los proveedores de almacenamiento en la nube se ven afectados, ya que actualmente la empresa tiene sus servidores principales en la nube. **Consecuencias:** Paralización de las operaciones de la compañía, Entorpecimiento de las tareas de los ejecutivos de ventas, La imagen de la compañía se ve afectada negativamente con los clientes, afectación de todas las operaciones de facturación **Frecuencia de ocurrencia:** el evento se puede producir 1 vez a lo largo de 12 meses. **Costo** puede llegar a ser de 14,427.22 $ solo se puede permitir una 1 hora este evento

34. Falla con Servicios de Proveedor de Almacenamiento en la Nube **Causa u origen** Se refiere a los servicios de proveedores en la nube en la cual la empresa tiene alojado la mayoría de sus servidores principales. **Consecuencias:** Paralización de las operaciones de la compañía, entorpecimiento de las tareas de los ejecutivos de ventas, la imagen de la compañía se ve afectada negativamente con los clientes, afectación de todas las operaciones de facturación. **Frecuencia de ocurrencia:** el evento se puede producir 1 vez a lo largo de 12 meses. **Costo** puede llegar a ser de 14,427.22 $ solo se puede permitir una 1 hora este evento.

35. Corrupción/Falla de Software de Maquina Virtuales **Causa u origen** Este riesgo se refiere al daño que puede sufrir una máquina virtual donde se aloje un sistema crítico, la restauración de las operaciones dependerá del tiempo que se tome poner en funcionamiento la máquina virtual o un respaldo de esta misma. **Consecuencias**: Paralización de las operaciones de la compañía, entorpecimiento de las tareas de los ejecutivos de ventas, la imagen de la compañía se ve afectada negativamente con los clientes, si esta no se puede levantar en tiempo y forma, en caso de que la corrupción se de en día de operaciones esto puede incurrir en perdida graves para la compañía por tiempo de inactividad. **Frecuencia de ocurrencia:** el

evento se puede producir 1 vez a lo largo de 12 meses. **Costo** .puede llegar a ser de 14,427.22 $ solo se puede permitir una 1 hora este evento.

36. Corrupción de Base de Datos SQL Server **Causa u origen** Se refiere al hecho que la base de datos que esta sobre SQL de Microsoft quede inhabilitada por cualquier motivo técnico, esto puede ser provocado por algún programa que se ejecute provocando conflictos con su funcionamiento, la eliminación de algún archivo de configuración, o el cambio de credenciales en un archivo de configuración, falta de espacio de almacenamiento, o el apagado incorrecto de la base de datos. **Consecuencias:** Paralización de las operaciones de la compañía, entorpecimiento de las tareas de los ejecutivos de ventas, la imagen de la compañía se ve afectada negativamente con los clientes, si esta no se puede levantar en tiempo y forma, en caso de que la corrupción se de en día de operaciones esto puede incurrir en perdida graves para la compañía por tiempo de inactividad, afectación a todos los procesos de ventas **Frecuencia de ocurrencia:** Nunca se ha presentado el evento. **Costo** puede llegar a ser de 14,427.22 $ solo se puede permitir una 1 hora este evento.

37. Corrupción de Base de Datos Oracle **Causa u origen** Se refiere al hecho que la base de datos que esta sobre Oracle quede inhabilitada por cualquier motivo técnico, esto puede ser provocado por algún programa que se ejecute provocando conflictos con su funcionamiento, la eliminación de algún archivo de configuración, o el cambio de credenciales en un archivo de configuración, falta de espacio de almacenamiento, o el apagado incorrecto de la base de datos. **Consecuencias:** Paralización de las operaciones de la compañía, entorpecimiento de las tareas de los ejecutivos de ventas, la imagen de la compañía se ve afectada negativamente con los clientes, si esta no se puede levantar en tiempo y forma, en caso de que la corrupción se de en día de operaciones esto puede incurrir en perdida graves para la compañía por tiempo de inactividad. **Frecuencia de ocurrencia:** Nunca se ha presentado el evento. **Costo** puede llegar a ser de 14,427.22 $ solo se puede permitir una 1 hora este evento.

38. Corrupción de Base de Respaldos Datos SQL Server **Causa u origen** El riesgo está dirigido a los respaldos de la base de datos SQL Server, los cuales pueden corromperse debido a que no se hicieron adecuadamente o a falta de espacio de almacenamiento. **Consecuencias**: no incurre directamente en las operaciones de facturación de la compañía, pero implican un alto riesgo de poder no poder restaurar las operaciones en caso de la corrupción de estas, perdida de información crítica de la compañía **Frecuencia de ocurrencia:** Nunca se ha presentado el evento. **Costo** no tiene costo sobre las operaciones de facturación

39. Corrupción de Base de Respaldos Datos Oracle **Causa u origen** El riesgo está dirigido a los respaldos de la base de datos Oracle, los cuales pueden corromperse debido a que no se hicieron adecuadamente o a falta de espacio de almacenamiento. **Consecuencias** no incurre directamente en las operaciones de facturación de la compañía, pero implican un alto riesgo de poder no poder restaurar las operaciones en caso de la corrupción de estas, perdida de información crítica **Frecuencia de ocurrencia:** Nunca se ha presentado el evento. **Costo** no tiene costo sobre las operaciones de facturación.

40. Falta/Falla de Respaldos de los sistemas principales **Causa u origen** El riesgo está dirigido a los respaldos de sistemas principales, los cuales pueden corromperse debido a que no se hicieron adecuadamente o a falta de espacio de almacenamiento. **Consecuencia:** Perdida de información de ventas**,** perdida de información crítica de la empresa, el evento no tiene afectación directa sobre los procesos de ventas. **Frecuencia de ocurrencia:** Esto puede ocurrir 1 vez cada 3 meses. **Costo** no tiene costo

41. Falta/Falla de Respaldos de Máquinas Virtuales **Causa u origen** El riesgo está dirigido a los respaldos de base de máquinas virtuales, los cuales pueden corromperse debido a que no se hicieron adecuadamente o a falta de espacio de almacenamiento. **Consecuencias:** Perdida de información de ventas, perdida de

información crítica de la empresa, el evento no tiene efecto sobre los procesos de ventas **Frecuencia de ocurrencia:** el evento se puede producir 2 al mes. **Costo** no tiene afectación en los procesos de ventas

42. Falta/Falla de Respaldos de Bases de Datos **Causa u origen** El riesgo está dirigido a los respaldos de bases de Datos., los cuales pueden corromperse debido a que no se hicieron adecuadamente o a falta de espacio de almacenamiento. **Consecuencias:** Perdida de información de ventas, perdida de información crítica de la empresa, el evento no tiene efecto sobre los procesos de ventas. **Frecuencia de ocurrencia:** el evento se puede producir 2 al mes. **Costo** no tiene afectación en los procesos de ventas

43. Espacio de almacenamiento insuficiente **Causa u origen** Debido al gran volumen de información que se ocupa para almacenar operaciones, respaldos de sistemas críticos, máquinas virtuales y documentos, este se encuentra limitado por el espacio que se pueda adquirir en la nube o los medios físicos de almacenamiento físicos que se puedan comprar. **Consecuencias**: Perdida de información, paralización de los sistemas informáticos que sustentan las operaciones críticas de la empresa, paralización de las bases de datos que sustentan las operaciones críticas de la empresa, afectación de las operaciones de facturación **Frecuencia de ocurrencia:** el evento se puede producir 2 al mes, con una duración de 30 minutos **Costo** El costo 7213 $.

44. Manejo inadecuado de datos críticos **Causa u origen** Envió de información de precios, descuentos y bonificaciones a personal ajeno a la compañía o que ha dejado de laborar en la empresa, esta información solo solamente es apta por la gerencia de la compañía, área de ventas y área financiera de la compañía. **Consecuencias:** Información crítica de la compañía puede caer en manos equivocadas. **Frecuencia de ocurrencia:** se da 1 vez todos los meses. **Costo** no tiene afectación en los proceso de ventas

45. Violación a derechos de autor **Causa u origen** Esto es ocasionado por la falta de licenciamiento de programas que son instalados en los equipos sistemas operativos o MS de Office. **Consecuencias:** Demandas legales contra la compañía y posibles sanciones económicas por consecuencia. **Frecuencia de ocurrencia:** Solo ha habido una advertencia debido a este problema, pero se solución, por ende, una demanda formal no ha habido. **Costo** será equivalente a la demanda, pero no se ha dado, no tiene afectación sobre el monto de venta.

46. Falta de mantenimiento físico a los equipos informáticos **Causa u origen** se refiere a no realizar mantenimientos preventivos a los equipos de cómputo, Smartphone, handhelds, servidores y sistemas de respaldos de energía. **Consecuencias:** Degradación de la calidad de funcionamiento de los equipos a los cuales no se les da mantenimiento, Costos asociados con la reparación de los equipos a los cuales no se les proporcione el mantenimiento adecuado. **Frecuencia de ocurrencia:** Nunca se ha presentado el evento.

47. Falta de actualización de software (Sistemas críticos, antivirus, herramientas de MS Office) **Causa u origen** Se refiere al hecho de no tener los recursos, licencias para poder hacer las actualizaciones de software a los sistemas críticos, antivirus, ya sea por problemas con el hardware, licencias. **Consecuencias:** No tiene efecto sobre las operaciones de ventas, sin embargo representa una vulnerabilidad sobre los sistemas y servicio afectados.

Frecuencia de ocurrencia: El evento se produce 4 veces al mes, esto con el ERP principal de la compañía.

48. Acceso no autorizado a sistemas externos **Causa u origen** Se refiere al hecho que los usuarios tengan acceso a sistemas externos de la compañía, sin la debida autorización. **Consecuencias:** Personal externo, puedan tener acceso a sistemas externos que contengan información del personal de la compañía. **Frecuencia de ocurrencia:** nunca se ha presentado el evento.

49. Acceso no autorizado a sistemas internos **Causa u origen** Esto se refiere a que los usuarios tengan acceso a sistemas internos fuera de la competencia de actividades de cada usuario o que alguien ajeno a la compañía tenga acceso no autorizado. **Consecuencias:** Personal externo, puedan tener acceso a sistemas internos que contengan información del personal de la compañía. **Frecuencia de ocurrencia:** nunca se ha presentado el evento

50. Red cableada expuesta para el acceso no autorizado **Causa u origen** Esto se refiere al acceso a personal no autorizado a la red cableada. **Consecuencias:** Ataques de tipo cibernético que afecten las operaciones de la compañía de manera negativa, robo de información crítica de la compañía, daño de la imagen de la compañía frente a sus clientes. **Frecuencia de ocurrencia:** nunca se ha presentado el evento

51. Red inalámbrica expuesta al acceso no autorizado **Causa u origen** Esto se refiere a la vulnerabilidad de la red inalámbrica, ya que, por su naturaleza, se toman las medidas correspondientes para evitar que cualquier persona pueda acceder a esta. **Consecuencias:** Ataques de tipo cibernético que afecten las operaciones de la compañía de manera negativa, robo de información crítica de la compañía, daño de la imagen de la compañía frente a sus clientes. **Frecuencia de ocurrencia:** nunca se ha presentado el evento

52. Dependencia a servicio técnico externo **Causa u origen** En este caso se refiere a las actividades propias de la gerencia de tecnología que dependan de personal ajeno a la gerencia, esto se da más en actividades del CEDI Norte, ya que por la distancia y no tener personal de TIC se recurre al jefe de transporte del CEDI Norte. **Consecuencias:** Esto genera un costo adicional a la gerencia de tecnología y comunicaciones, no tiene afectaciones sobre los procesos de facturación. **Frecuencia de ocurrencia:** El evento se ha producido 2 entre 7 meses al año, solo se realiza con trabajos específicos como creación de nuevos puertos de red, o algún

soporte para una determinada plataforma o implementación de algún sistema nuevo, **Costo** el costo de este tipo de evento puede variar puede rondar entre los 100 $.

53. Robo (físico) Smartphone **Causa u origen** este riesgo se refiere al hurto de equipos de smartphones asignados a los ejecutivos de ventas. Consecuencias costos asociados con el reemplazo de los equipos. **Consecuencias** Costos asociados con el reemplazo de los equipos, perdida de información relacionada con las actividades de facturación Retraso de las actividades de los ejecutivos de ventas. **Frecuencia de ocurrencia** este evento no es muy frecuente se han reemplazado 4 equipos a los largo por este concepto de un año. **Costo** el costo del equipo seria alrededor de los 290 $, equivalente a 1160.

54. Robo (Físico) PDA **Causa u origen** este riesgo se refiere al hurto de equipos PDA, en este caso las PDA ya se dejaron de utilizar, en su totalidad. **Consecuencias:** Costos asociados con el reemplazo del equipo. **Frecuencia de ocurrencia:** no se evalúa ya que la PDA ha sido descartada.

55. Robo (físico) Computadora Laptop **Causa u origen** este riesgo se refiere al hurto de equipos de computador laptops asignados a los supervisores de ventas. Consecuencias costos asociados con el reemplazo de los equipos y retraso de las actividades de los supervisores de ventas. **Consecuencias:** Costos asociados con el reemplazo del equipo, perdida de información relacionada con las actividades de facturación, retraso de las actividades de los ejecutivos de ventas. **Frecuencia de ocurrencia:** este evento no es muy frecuente se han reemplazado 1 equipo del año por este concepto. **Costo** el costo del equipo laptop 1200 $, la operación de ventas se vio afectada 8 horas con un costo de venta 1576 $

56. Falla con la plataforma de almamater **Causa u origen** esto se debe a problemas con el servicio que proporciona almamater, el cual sirve como plataforma para interactuar con la cadena supermercados walmart. **Consecuencias** Incumplimiento

con los pedidos de la cadena de supermercados walmart, el cual es un importante cliente para la empresa **Frecuencia de ocurrencia** 1 cada 2 años, por acuerdos, lo máximo que puede durar es 1 hora. **Costo** 2125 $ por la duración del evento.

57. Robo (físico) Tablet **Causa u origen** este riesgo se refiere al hurto de equipos de tablets asignadas a gerentes y/o algunos supervisores de ventas. **Consecuencias** Costos asociados con el reemplazo de los equipos, perdida de información relacionada con las actividades de facturación, retraso de las actividades de los ejecutivos de ventas. **Frecuencia de ocurrencia:** este evento tiene más de 3 años sin suceder. **Costo:** Costo de una Tablet es 200 $.

En conjunto con la gerencia de tecnología y comunicaciones se procedió a crear las tablas de criterios de consecuencias, criterios de probabilidad adoptando el formato de las tablas de la sección 6.1

9.4.1 CRITERIOS DE PROBABILIDAD

El criterio de probabilidad se establece según las veces que un evento se presenta al mes, ente mayor sea la cantidad de veces el indicar se elevara más, el criterio de frecuencia se establece con el siguiente cuadro de criterios:

Tabla 9 Criterios de Frecuencia de Ocurrencia de incidentes

Frecuencia	Descripción	Valor
Alta	El evento se presenta más de 4 veces al mes	4
Media	El evento probablemente se presente 2 veces al mes	3
Muy Bajo	El evento podría ocurrir en cualquier momento en los próximos 3 o 4 meses	2
Bajo	Nunca se ha presentado el evento	1

9.4.2 CRITERIOS DE IMPACTO

El criterio de impacto se establece según la gravedad que representa para las operaciones al presentarse un evento, entre más grave sea el impacto de los eventos sobre las operaciones de facturación más alto será el indicador.

Tabla 10 Criterios de impacto de daño

Impacto	Descripción	Valor
Critico	• Paralización de las operaciones de ventas de la compañía o el tiempo que trascurre la jornada laboral de la empresa. • El evento podía incurrir en pérdidas económicas o un gasto a la compañía mayor a los 10,000 $ • Insatisfacción con los clientes más importantes (aquellos que compran en grandes cantidades de productos y/o horarios establecidos de entrega o atención) o con la totalidad de ellos, que implique devolución de los productos o la no realización de compromisos de ventas. • Perdida de información crítica de la empresa • El evento afecta a todos procesos de facturación	4
Alto	• Perdidas Económicas graves o un gasto equivalente (2,000 $ a 10,000 $) • Insatisfacción con los clientes • Efecto negativo en la imagen de la empresa, por falta de información precisa en los equipos o falta de acceso a ella para poder atender a los clientes. • Las operaciones de facturación se afectadas en la jornada laboral en entre 2 a 4 horas. • La información que solo concierne a la compañía se ve comprometida o expuesta • El evento afectado al menos dos procesos de facturación	3

Medio	• Efecto negativo en la imagen de la empresa • Perdidas Económicas moderadas o un gasto moderado (menos o igual a 2000 $) • Las operaciones de ventas se afectan por menos de 1 una hora. • El evento afecta de 2 a 3 ejecutivos de ventas	2
Bajo	• No hay efectos negativos para la compañía • Las operaciones de ventas no se ven afectadas • El evento afecta a un ejecutivo de venta • El evento tiene una duración de menos de una hora	1

9.4.3 NIVEL DE RIESGO

Tabla 11 Acción requerida (marco de tiempo para bajar el nivel de riesgo)

Nivel de Riesgo	Acción requerida
CRITICO	***Acción requerida de inmediato***: El evento no debe de proceder hasta que se someta a las medidas necesarias para reducir el nivel de riesgo tan bajo como sea razonablemente posible.
ALTO	***Acción requerida hoy :*** El evento puede continuar, siempre que: • El nivel de riesgo sea reducido tan bajo como sea razonablemente posible • Siempre que se supervise que estos tratamientos se lleven a cabo. •La evaluación del riesgo ha sido revisada y aprobada por los jefes de área. •Los jefes de área debe de revisar y documentar la efectividad de los controles de riesgo implementados.
MEDIO	***Acción requerida de esta semana :*** El evento sólo puede continuar, siempre que: • El nivel de riesgo sea reducido a un nivel tan bajo como sea razonablemente posible. • Se ha preparado un procedimiento o método de trabajo seguro para tratar el riesgo.

BAJO	***Acción requerida de este mes :*** Se ha preparado un procedimiento o método de trabajo seguro para tratar el riesgo

9.4.4 MATRIZ DE ANÁLISIS DE RIESGOS

Una vez concluida la tabla de acción requerida (Tabla 10: Acción requerida (marco de tiempo para bajar el nivel de riesgo) , se procedió con la construcción de la tabla de valores para el cálculo de riesgo (Tabla 11: Valores para el cálculo de riesgo), que es un requisito indispensable para poder crear una matriz de evaluación de riesgo la tabla contiene tres casillas: Una de riesgo, la otra de valor de frecuencia y la ultima de valor de magnitud, dicha tabla fue impresa y entregada junto con las tablas de Tabla 9: Criterios de Magnitud de Daño y de criterio de frecuencia ***(***Tabla 8: Criterios de Frecuencia de Ocurrencia de incidentes***)*** con la cual se apoyaron para completar las casillas de valores de consecuencias y valores de probabilidad de la tabla. se les explico la forma de completar esta tabla siguiendo los pasos como se muestra a continuación:

- ***Paso numero1***: de la lista de riesgo de la Tabla 11: Valores para el cálculo de riesgo, tome la tabla de Tabla 9: Criterios de Magnitud de Daño, escoja la clasificación de criterio de magnitud más adecuada para cada riesgo anotado el valor de su puntuación en la casilla en blanco de valor de consecuencia así sucesivamente con cada uno de los riesgos de la lista de la Tabla 11: Valores para el cálculo de riesgo.
- ***Paso numero 2:*** con la tabla de la Tabla 3 de criterio de frecuencia, escoja la frecuencia más adecuada de cada riesgo y anótela en la casilla en blanco de valor de probabilidad de la tabla de la Tabla 4 sucesivamente hasta completar toda la tabla 11.

Tabla 12 Valores para el cálculo de riesgo

NO RIESGO	DESCRIPCION	Probabilidad	Magnitud

1	Falla en sistemas de facturación	3	2
2	Daño en batería (respaldo ups)	2	2
3	Fallo en equipo de computadora oficina	1	2
4	Falla en los servicios de internet	2	3
5	Fallo en sistema POS (Sistema del banco)	2	2
6	Carga en batería de celular (se agota rápidamente)	2	1
7	Ataque físico a los equipos informáticos	1	2
8	Ataque informático	4	4
9	Daños por vandalismo	1	1
10	Fraude (Estafa)	1	2
11	Robo (físico) Computadoras PC	1	1
12	Infección de virus informático	4	3
13	Sismos	4	4

14	Polvo en los equipos informáticos	4	1
15	Falla Fluido eléctrico	4	1
16	Mal manejo de sistemas y herramientas informáticas	2	1
17	Utilizar programas no autorizado	1	1
18	Unidades portables sin cifrado	1	1
19	Manejo inadecuado de contraseñas (inseguras, no cambiar)	2	1
20	Transmisión de contraseñas por medios no oficiales	3	1
21	Compartir contraseñas o permisos a terceros no autorizados	4	1
22	Exposición o extravío de equipo, unidades de almacenamiento	1	1
23	Falla de sistema principal(ERP Principal)	2	3
24	Falla en Herramientas de MS Office	1	1
25	Falla/Daño en los smartphones	1	2
26	Falla/Daño en Impresoras Móviles	1	2

27	Falla/Daño en Impresoras Fijas	1	2
28	Falla/Daño en Físico Tablet	1	1
29	Falla/Daño en Físico en PDA	1	1
30	Falla/Daño Físico en Computadora táctil	2	3
31	Falla en la Infraestructura interna de Red	1	2
32	Falla de Paquete de Servicios de Internet Móvil	2	4
33	Falla de Paquete de Servicios de Internet Corporativo	2	4
34	Falla con Servicios de Proveedor de Almacenamiento en la Nube	2	4
35	Corrupción/Falla de Software de Maquina Virtuales	1	4
36	Corrupción de Base de Datos SQL Server	1	4
37	Corrupción de Base de Datos Oracle	1	4
38	Corrupción de Base de Respaldos Datos SQL Server	1	1
39	Corrupción de Base de Respaldos Datos Oracle	1	1

40	Falta/Falla de Respaldos de los sistemas principales.	1	1
41	Falta/Falla de Respaldos de Máquinas Virtuales	1	1
42	Falta/Falla de Respaldos de Bases de Datos.	1	1
43	Espacio de almacenamiento insuficiente	3	3
44	Manejo inadecuado de datos críticos	2	4
45	Violación a derechos de autor	1	1
46	Falta de mantenimiento físico a los equipos informáticos	1	1
47	Falta de actualización de software	4	1
48	Acceso no autorizado a sistemas externos	1	1
49	Acceso no autorizado a sistemas internos	1	1
50	Red cableada expuesta para el acceso no autorizado	1	3
51	Red inalámbrica expuesta al acceso no autorizado	1	3
52	Dependencia a servicio técnico externo	2	1

53	Robo (físico) Smartphone	2	1
54	Robo (Físico) PDA	1	1
55	Robo (físico) Computadora Laptop	1	2
56	Falla del sistema de almamater	2	3
57	Robo (Físico) Tablet	1	1

Con los valores de la tabla de la Tabla 11: Valores para el cálculo de riesgo, se procederá a construir la matriz de riesgo tomada del formato de la tabla de Ilustración 4: Matriz de evaluación de riesgo, donde las puntuaciones de frecuencia y magnitud serán ubicados siguiente tabla para indicar el nivel de riesgo.

Tabla 13 Matriz de Evaluación de riesgos

			GRAVEDAD (IMPACTO)			
			BAJO	MEDIO	ALTO	CRITICO
			1	2	3	4
APARICIÓN (probabilidad)	ALTA	4				
	MEDIA	3				
	MUY BAJA	2				
	BAJA	1				

Tabla 14 Riesgos en la matriz de riesgos

			GRAVEDAD (IMPACTO)			
			BAJO	MEDIO	ALTO	CRITICO
			1	2	3	4
Frecuencia (probabilidad)	ALTA	**4**	14,15,21,47		12	8,13
	MEDIA	**3**	20,45	1	43	
	MUY BAJA	**2**	6,7,16,19,52,53	2,5	4,23,30,56	32,33,34,44,,35
	BAJA	**1**	9,11,17,18,22,1,24,28,29,40, 41,42,45,46,48,49,54,57,38, 39	3,10,25,26,27,31,55	50,51	36,37

Al observar la matriz evaluación de riesgo podemos notar que los riesgos están distribuidos de la siguiente manera:

En el nivel crítico se encontraron riesgos

- Ataque informático
- Virus
- Sismos

En el nivel alto se encontraron

- Falla en sistemas de facturación
- Falla en los servicios de internet
- Falla de sistema principal.
- Falla/Daño Físico en Computadora táctil
- Falla de Paquete de Servicios de Internet Móvil
- Falla de Paquete de Servicios de Internet Corporativo
- Falla con Servicios de Proveedor de Almacenamiento en la Nube
- Espacio de almacenamiento insuficiente
- Manejo inadecuado de datos críticos
- Falla del sistema de almamater
- Falla de software de máquinas virtuales

En el nivel medio se encontraron

- Daño en batería (respaldo ups)
- Fallo en sistema POS (Sistema del banco)
- Polvo en los equipos informáticos
- Falla Fluido eléctrico
- Transmisión de contraseñas por medios no oficiales
- Compartir contraseñas o permisos a terceros no autorizados
- Corrupción de Base de Datos SQL Server
- Corrupción de Base de Datos Oracle
- Corrupción de Base de Respaldos Datos SQL Server
- Corrupción de Base de Respaldos Datos Oracle
- Falta de actualización de software
- Red cableada expuesta para el acceso no autorizado
- Red inalámbrica expuesta al acceso no autorizado

Nivel Bajo

- Fallo en equipo de computadora oficina
- Ataque físico a los equipos informáticos
- Daños por vandalismo
- Robo (físico) Computadoras PC
- Malmanejo de sistemas y herramientas informáticas
- Unidades portables sin cifrado
- Exposición o extravío de equipo, unidades de almacenamiento
- Falla en Herramientas de MS Office
- Falla/Daño en Impresoras Móviles
- Falla/Daño en Físico Tablet

- Falta/Falla de Respaldos de Máquinas Virtuales
- Violación a derechos de autor
- Acceso no autorizado a sistemas internos

9.4.5 RECOMENDACIONES PARA MITIGAR EL RIESGO

Se procedió a realizar una reunión en el CEDI Matriz de OCAL SA, para analizar los resultados de la matriz de riesgos en conjunto con personal de la Gerencia de Tecnología y comunicaciones de la empresa, así como con los jefes de área del departamento de soporte técnico y el departamento de desarrollo e integración de sistemas, en esta caso la Gerencia de Tecnología y comunicaciones prioriza aquellos riesgos que considera que pueden entorpecer o atentar contra las operaciones de facturación de la compañía OCAL SA, en este caso se priorizara los riegos cuyo nivel de riesgo sea crítico y alto, de acuerdo a la Tabla 13.

Para los temas de nivel crítico se tomarán medidas de acuerdo a los lineamentos de la Gerencia de Tecnología y las necesidades de la compañía con respecto a las operaciones de facturación.

Por tal motivo se enumeran a continuación todos aquellos riesgos en los cuales se describirán medidas o acciones a tomar:

Ataque informático

Virus

Sismos

Falla en sistemas de facturación

Falla en los servicios de internet

Falla de sistema principal.

Falla/Daño Físico en Computadora táctil

Falla de Paquete de Servicios de Internet Móvil

Falla de Paquete de Servicios de Internet Corporativo

Falla con Servicios de Proveedor de Almacenamiento en la Nube

Espacio de almacenamiento insuficiente

Manejo inadecuado de datos críticos

Falla del sistema de almamater

Corrupción o falla de máquinas virtuales

9.4.5.1 Tratamiento de los riesgos

Ataque informático y virus: Se deben de mantener las medidas de seguridad actuales, al mismo tiempo comunicar medidas a los usuarios para mantener a salvo los equipos informáticos de cualquier amenaza de ataque informático o virus.

Sismos: Al ser un evento natural impredecible cualquier afectación es inevitable y adoptar herramientas informáticas o soluciones en caso de desastres.

Falla en sistemas de facturación: Establecer mejores procesos para la actualización de precios

Falla en los servicio de internet (Móvil y servicio de internet convencionales): La única medida a posible es hacer cumplir a los proveedores de los servicios con los contratos establecidos y hacer cumplir las clausulas las cuales cubren a OCAL en caso de cualquier inconveniente con el servicio. En el caso de los usuarios instruirlos que medidas deben de tomar en caso de que los servicios fallen.

Falla del sistema principal (ERP Principal): Las medidas a tomar serian mantener las actualizaciones del sistema principal al día. Así como realizar el mantenimiento adecuado a las distintas configuraciones (espacio en tablespace, espacio en memoria, variables de entorno de sistema) que requiera el sistema para mantenerse en óptimas condiciones.

Falla/Daño Físico en Computadora táctil: Este es un riesgo que se tiene q asumir, las regulaciones del aeropuerto Augusto Cesar Sandino no permiten tomar medidas más efectivas.

Falla de Paquete de Servicios de Internet Corporativo: Este es un riesgo que se tiene que asumir, como medidas a tomar serian la de hacer cumplir las clausulas por incumpliendo de contrato al proveedor y tener un servicio alternativo con un proveedor diferente para poder conectarse al proveedor de servicio de la nube desde ese enlace.

Falla con Servicios de Proveedor de Almacenamiento en la Nube: Este es un riesgo que se tiene que asumir, como medidas a tomar serian la de hacer cumplir las clausulas por incumpliendo de contrato al proveedor

Espacio de almacenamiento insuficiente: La gerencia de TIC debe de gestionar la compra de más espacio de almacenamiento tanto en la nube, como la compra de discos duros para los servidores locales.

Falla del sistema de almamater: Este es un riesgo que se tiene que asumir, como medidas a tomar serian la de hacer cumplir las clausulas por incumpliendo de contrato al proveedor.

Manejo inadecuado de datos críticos: Establecer mejores controles para el acceso a la información, delimitar que personas o integrantes deben de tener acceso a determinada información.

Corrupción o falla de máquinas virtuales: La gerencia de TIC debe de gestionar la adquisición de servidores redundantes, para no afectar las operaciones de ventas.

IX. DISCUSION Y CONCLUSIONES

El diseño metodológico propuesto es la base que fundamenta el alineamiento de la norma **ISO 31000:2009,** mediante el desarrollo de Caso de estudio. El diseño y la conducción del Caso de estudio, se sustenta en técnicas de caso de estudio y la pertenencia del proceso de evaluación de riesgo del ISO, lo que permitió, contrastar la teoría en un contexto real.

El análisis los procesos de facturación de la empresa OCAL S.A, se desarrolló principalmente mediante revisión documental y entrevistas a los actores principales, esto ayudó a entender la forma en que operan los procesos de facturación y las tecnologías que soportan dichos procesos y de esta forma evaluar el riesgo.

El estudio de análisis de riesgo permitió identificar y clasificar los riesgos, así como sus consecuencias y ocurrencias para luego proponer tratamientos para disminuir su impacto. Los hallazgos fueron validados con los participantes con el propósito de conocer si la suficiente evidencia ha sido recolectada y analizada, en la forma validación se sustenta el consenso de los participantes.

X. RERENCIAS

(IEC), I. E. (2009). *Risk managemet - Risk Assessment techniques.*

(2011). En *Indian Standard RISK MANAGEMENT — PRINCIPLES AND GUIDELINES*. NEW DELHI.

ADELAIDE, U. o. (s.f.). Obtenido de http://www.adelaide.edu.au/legalandrisk/docs/resources/Risk_Matrix.pdf

Adelaidem, I. (2009). *Risk management - Principles guidelines NTC-ISO 31000.*

Adelaidem, U. o. (2009). *RISK MANAGEMENT HANDBOOK, AS/NZS ISO 31000:2009 Risk Management.*

Becker, H. O. (s.f.). Enciclopedia internacional de las Ciencias Sociales T.3. Mauhnundrid, Aguilar.

Castro, A. R. (2017). Riesgo tecnológico y su impacto para las organizaciones. *Seguridad Cultura de Prevencion para TI.*

ICONTEC. (2014). *GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES.* Instituto Colombiano de Normas Técnicas y Certificación.

ISO. (s.f.). *About ISO*. (ISO) Obtenido de http://www.iso.org/iso/home/about.htm

Zapata, S. (16 de Mayo de 2013). *http://seminariomonografico.blogspot.com/2013/05/como-redactar-la-metodologia-o-diseno.html*.

XI. ANEXOS

ANEXO 1. CUESTIONARIO PARA EJECUTIVOS DE VENTAS

IMPORTADORA Y DISTRIBUIDORA OCAL .SA

DEPARTAMENTO DE DESARROLLO E INTEGRACION DE SISTEMAS

El siguiente cuestionario, tiene como propósito recopilar información de incidentes relacionados con las herramientas tecnológicas ocupadas en el área de ventas, para realizar un análisis de riesgos en los procesos de ventas.

I. DATOS PERSONALES

Nombre Completo:	
Edad:	
Cargo que desempeña:	
Tiempo que tiene de trabajar para la empresa	

II. GLOSARIO DE DEFINICIONES

Se define como **riesgo** al efecto de desviación de aquello que se espera, sea positivo o negativo.

Se define como **incidente**: Un evento puede ser una o más ocurrencias, y puede tener varias causas

III. CUESTIONARIO

1. ¿Cuáles son las metas/objetivos designados para que realice sus funciones?

_____.

_____.

2. ¿Qué dispositivos y/o sistemas tecnológicos utiliza para realizar sus funciones en el área de ventas? (Puede marcar más de una opción)

Dispositivos/Tecnologías	**Sistemas/Software**
☐ Tablet	☐ Sistema y Servicios Móviles "SYSMO"
☐ Smartphone	☐ JD Edwards "JDE"
☐ PDA	☐Enterprise Warehouse Management System "EWMS"
☐ Computador(laptop)	☐ Sistema POS (BAC)
☐ GPS(Garmin)	☐Evolution
☐ Impresoras	☐ Sistema de Atención a Colaboradores "SAC
	☐ MS Office
	☐ Sistema POS OCAL

3. ¿Cómo se define su carga de trabajo?

☐Planificación: Entregada por superior inmediato.

☐Atención diaria de incidentes.

☐Sin planificación

☐Otro, especifique

4. ¿Cuáles son los incidentes presentados en el área de ventas relacionados con los dispositivos y/o sistemas tecnológicos? ? (Puede marcar más de una opción)

Dispositivos	Sistemas
☐ Daño del equipo	☐ Pérdida de datos
☐ Robo (Hurto Físico)	☐Falla de Paquete de Servicios de Internet
☐ Ataques de Virus	☐ Falla en los sistemas
☐ Daño en Impresora	☐ Otros, especifique
☐ Otros, especifique	

5. Indique la frecuencia de ocurrencia de incidentes relacionados con los dispositivos y/o sistemas tecnológicos (Marque la frecuencia con una X)

Criterios de Frecuencia de Ocurrencia de incidentes	
Alta	El evento se presenta más de 4 veces al mes
Media	El evento se presenta 2 veces al mes
Muy bajo	El Evento ocurre eventualmente, podría ocurre al menos una vez al mes
Bajo	Nunca se ha presentado el evento

Daño del equipo				
Robo (Hurto Físico)				
Ataques de Virus				
Daño en Impresora				
Pérdida de datos				
Falla en los sistemas				
Falla de Paquete de Servicios de Internet				

6. ¿Cuál es la magnitud del daño que pueden provocar estos riesgos, en sus operaciones? (Marque la frecuencia con una X)

Criterios de Frecuencia de Ocurrencia de incidentes	
Critico	Paralización de las operaciones de ventas Perdida/Insatisfacción de los clientes Efecto negativo en la imagen de la empresa Perdidas económicas
Media	Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa

	Las operaciones de ventas se encuentran paralizadas más de 2 días
Muy Bajo	Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa Las operaciones de ventas se encuentran paralizadas durante medio día
Bajo	No hay efectos negativos para la compañía Las operaciones de ventas no se ven afectadas

Daño del equipo				
Robo (Hurto Físico)				
Ataques de Virus				
Daño en Impresora				
Pérdida de datos				
Falla en los sistemas				
Falla de Paquete de Servicios de Internet				

7. En el caso de un incidente relacionado con los dispositivos y/o sistemas tecnológicos, ¿Cuánto estima que ascienden sus pérdidas de venta por día?

☐ 0 - $100

☐ $101 - $200

☐ $201 - $300

☐ Más de $300

ANEXO 2. TÉCNICOS DE SOPORTE TÉCNICO

IMPORTADORA Y DISTRIBUIDORA OCAL .SA

DEPARTAMENTO DE DESARROLLO E INTEGRACIÓN DE SISTEMAS

El siguiente cuestionario tiene como propósito recopilar información de incidentes relacionados con las herramientas tecnológicas ocupadas en el área de ventas, para realizar un análisis de riesgos en los procesos de ventas.

I. DATOS PERSONALES

Nombre Completo:	
Edad:	
Cargo que desempeña:	

Tiempo que tiene de trabajar para la empresa	

II. GLOSARIO DE DEFINICIONES

Se define como **riesgo** al efecto de desviación de aquello que se espera, sea positivo o negativo.

Se define como **incidente**: Un evento puede ser una o más ocurrencias, y puede tener varias causas

III. CUESTIONARIO

1. **¿Cuáles son las tecnologías que se utilizan para dar apoyo a las operaciones de ventas**
2. **¿Cuáles son los incidentes más comunes presentados en el área de ventas relacionados con los dispositivos y/o sistemas tecnológicos**
3. **Indique la frecuencia de ocurrencia de incidentes relacionados con los dispositivos y/o sistemas tecnológicos.**
4. **¿Cuál es la magnitud del daño que pueden provocar estos riesgos?**

ANEXO 3. JEFES DE DEPARTAMENTO DE TECNOLOGIA

IMPORTADORA Y DISTRIBUIDORA OCAL .SA

DEPARTAMENTO DE DESARROLLO E INTEGRACIÓN DE SISTEMAS

El siguiente cuestionario tiene como propósito recopilar información de incidentes relacionados con las herramientas tecnológicas ocupadas en el área de ventas, para realizar un análisis de riesgos en los procesos de ventas.

I. DATOS PERSONALES

Nombre Completo:	
Edad:	

Cargo que desempeña:	
Tiempo que tiene de trabajar para la empresa	

II. GLOSARIO DE DEFINICIONES

Se define como **riesgo** al efecto de desviación de aquello que se espera, sea positivo o negativo.

Se define como **incidente**: Un evento puede ser una o más ocurrencias, y puede tener varias causas

III. CUESTIONARIO

1. **¿Cuáles son los objetivos/metas definidos por la organización?**
2. **¿Cuál es el giro del negocio en que desarrolla la organización o compañía?**
3. **¿Cuáles son objetivos del de la Gerencia de Tecnología e información'**
4. **¿Cuáles son las funciones del área de soporte técnico?**
5. **¿Cuáles son las funciones del área de desarrollo de integración y sistemas?**
6. **¿Cuáles son las tecnologías de la información asociadas a los procesos de facturación de la compañía?**
7. **¿Cuáles son los riesgos de las tecnologías de la información asociadas con los procesos de facturación?**
8. **¿Cuáles son las causas y posibles consecuencias de los de las tecnologías de la información asociadas con los procesos de facturación?**
9. **¿Cuál es la probabilidad de ocurrencia de los riesgos?**
10. **¿Cómo se identifican los riesgos de las tecnologías de la información asociadas con los procesos de facturación?**
11. **¿Cuáles son las fuentes de los riesgos de las tecnologías de la información asociadas con los procesos de facturación?**
12. **¿Qué roles (cargos) están definidos en la Gerencia de Tecnología e información?**
13. **¿Cómo se define la carga en la Gerencia de Tecnología e información?**
14. **¿Cuál es el origen de estos riesgos?**

15.¿Qué consecuencias resultan de estos riesgos?

16.¿En un mes con qué frecuencia ocurren estos riesgos?

ANEXO 4. MUESTRAS DE ENTREVISTAS REALIZADAS

Entrevista a Ejecutivo de Ventas

IMPORTADORA Y DISTRIBUIDORA OCAL .SA

DEPARTAMENTO DE DESARROLLO E INTEGRACION DE SISTEMAS

El siguiente cuestionario, tiene como propósito recopilar información de incidentes relacionados con las herramientas tecnológicas ocupadas en el área de ventas, para realizar un análisis de riesgos en los procesos de ventas.

I. DATOS PERSONALES

Nombre Completo:	Rolando J. Soto Romero
Edad:	24
Cargo que desempeña:	Asesor de Ventas de Calle
Tiempo que tiene de trabajar para la empresa	36 meses.

II. GLOSARIO DE DEFINICIONES

Se define como **riesgo** al efecto de desviación de aquello que se espera, sea positivo o negativo.

Se define como **incidente**:Un evento puede ser una o más ocurrencias , y puede tener varias causas

III. CUESTIONARIO

1. **¿Cuáles son las metas/objetivos designados para que realice sus funciones?**

2. **¿Qué dispositivos y/o sistemas tecnológicos utiliza para realizar sus funciones en el área de ventas? (Puede marcar más de una opción)**

Dispositivos/Tecnologías	Sistemas/Software
☐ Tablet	☑ Sistema y Servicios Móviles "Sysmo"
☑ Smartphone	☑ JD Edwards "JDE"
☐ PDA	☐ Enterprise Warehouse Management System "EWMS"
☐ Computador(laptop)	☐ Sistema POS (BAC)
☐ GPS(Garmin)	☐ Evolution
☑ Impresoras	☐ Sistema de Atención a Colaboradores "SAC
	☐ MS Office
	☐ Sistema POS OCAL

3. **¿Cómo se define su carga de trabajo?**

☑ Planificación: Entregada por superior inmediato.
☐ Atención diaria de incidentes.
☐ Sin planificación
☐ Otro, especifique

4. **¿Cuáles son los incidentes presentados en el área de ventas relacionados con los dispositivos y/o sistemas tecnológicos? ? (Puede marcar más de una opción)**

Página **1** de **2**

Gerencia de TIC

Dispositivos	Sistemas
☐ Daño del equipo	☑ Pérdida de datos
☐ Robo (Hurto Físico)	☑ Falla de Paquete de Servicios de Internet
☑ Ataques de Virus	☑ Falla en los sistemas.
☐ Daño en Impresora	☐ Otros, especifique → en el safe browser.
☐ Otros, especifique	

5. Indique la frecuencia de ocurrencia de incidentes relacionados con los dispositivos y/o sistemas tecnológicos(Marque la frecuencia con una X)

Criterios de Frecuencia de Ocurrencia de incidentes	
Alta	El evento se presenta más de 4 veces al mes
Media	El evento se presenta 2 veces al mes
Muy Bajo	El Evento ocurre eventualmente, podría ocurre al menos una vez al mes
Bajo	Nunca se ha presentado el evento

Dispositivos	Muy Baja	Baja	Media	Alta
Daño del equipo				
Robo (Hurto Físico)			✓	
Ataques de Virus				
Daño en Impresora				
Sistemas	**Muy Baja**	**Baja**	**Media**	**Alta**
Pérdida de datos				
Falla en los sistemas		✓	✓	
Falla de Paquete de Servicios de Internet				✓

6. ¿Cuál es la magnitud del daño que pueden provocar estos riesgos, en sus operaciones? (Marque la frecuencia con una X)

Criterios de Frecuencia de Ocurrencia de incidentes	
Critico	Paralización de las operaciones de ventas Perdida/Insatisfacción de los clientes Efecto negativo en la imagen de la empresa Perdidas económicas
Media	Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa Las operaciones de ventas se encuentran paralizadas más de 2 días
Muy Bajo	Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa Las operaciones de ventas se encuentran paralizadas durante medio día
Bajo	No hay efectos negativos para la compañía Las operaciones de ventas no se ven afectadas

Dispositivos	Critico	Alta	Mediana	Baja
Daño del equipo				
Robo (Hurto Físico)				
Ataques de Virus				
Daño en Impresora				
Sistemas	**Critico**	**Alta**	**Media**	**Baja**
Pérdida de datos				
Falla en los sistemas				
Falla de Paquete de Servicios de Internet				

7. En el caso de un incidente relacionado con los dispositivos y/o sistemas tecnológicos, ¿Cuánto estima que ascienden sus pérdidas de venta por día?

☑ 0 - $100
☐ $101 - $200
☐ $201 - $300
☐ Más de $300

Entrevistas a Técnico de Informática #1

IMPORTADORA Y DISTRIBUIDORA OCAL .SA

DEPARTAMENTO DE DESARROLLO E INTEGRACIÓN DE SISTEMAS

El siguiente cuestionario tiene como propósito recopilar información de incidentes relacionados con las herramientas tecnológicas ocupadas en el área de ventas, para realizar un análisis de riesgos en los procesos de ventas.

I. DATOS PERSONALES

Nombre Completo:	Norman José Arévalo Quiñonez
Edad:	24
Cargo que desempeña:	Auxiliar de Soporte Tecnico
Tiempo que tiene de trabajar para la empresa	2 Años

II. GLOSARIO DE DEFINICIONES

Se define como **riesgo** al efecto de desviación de aquello que se espera, sea positivo o negativo.

Se define como **incidente**: Un evento puede ser una o más ocurrencias , y puede tener varias causas

III. CUESTIONARIO

1. **¿Cuáles son las tecnologías que se utilizan para dar apoyo a las operaciones de ventas?(Puede marcar más de una opción)**

Dispositivos/Tecnologías	Sistemas/Software
☒ Tablet	☒ Sistema y Servicios Móviles "Sysmo"
☒ Smartphone	☒ JD Edwards "JDE"
☒ PDA	☒ Enterprise Warehouse Management System "EWMS"
☒ Computador(laptop)	☒ Sistema POS
☒ GPS(Garmin)	☐ Evolution
☒ Servidores Físicos	☐ Sistema de Atención a Colaboradores "SAC
☒ Infraestructura interna de Red	☒ MS Office
☒ Servicio de Alojamiento en la nube	☒ Bases de Datos SQL Server
☒ Servicio de Internet Corporativo	☒ Bases de Datos Oracle
☒ Impresoras Móviles	☐ Otros Especifique
☒ Impresoras Fijas	
☒ Servidores Virtuales	
☐ Otros Especifique	

2. **¿Cuáles son los incidentes más comunes presentados en el área de ventas relacionados con los dispositivos y/o sistemas tecnológicos? (Puede marcar más de una opción)**

Delincuencia Común
☒ Sabotaje (ataque físico y electrónico)
☒ Daños por vandalismo
☒ Fraude / Estafa
☒ Robo (físico) (Computadoras, Tablet, Smartphone, PDA)
☐ Robo de información electrónica
☐ Intrusión a Red interna
☒ Virus / Ejecución no autorizado de programas
☐ Violación a derechos de autor
Desastres Naturales
☐ Incendio
☒ Sismos
☒ Polvo
☐ Ventilación inadecuada
☒ Falla de fluido eléctrico
Responsabilidad de Usuario Final y decisiones institucionales
☐ Falta de inducción, capacitación y sensibilización sobre el uso herramientas tecnológicas
☒ Mal manejo de sistemas y herramientas
☒ Utilización de programas no autorizados / software 'pirateado'
☐ Falta de pruebas de software nuevo con datos productivos
☐ Pruebas del Software
☐ Pérdida de datos
☐ Manejo inadecuado de datos críticos (codificar, borrar)
☒ Unidades portables con información sin cifrado
☐ Transmisión no cifrada de datos críticos
☒ Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
☒ Compartir contraseñas o permisos a terceros no autorizados
☐ Transmisión de contraseñas por medios no oficiales
☒ Exposición o extravío de equipo, unidades de almacenamiento
☒ Sobrepasar autoridades
☐ Falta de definición de perfil, privilegios y restricciones del personal
☐ Falta de mantenimiento físico (proceso, repuestos e insumos)
☐ Falta de actualización de software (proceso y recursos)
☐ Fallas en permisos de usuarios (acceso a archivos)
☐ Acceso electrónico no autorizado a sistemas externos
☐ Acceso electrónico no autorizado a sistemas internos
☐ Red cableada expuesta para el acceso no autorizado
☐ Red inalámbrica expuesta al acceso no autorizado
☐ Dependencia a servicio técnico externo
☐ Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
☐ Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control
☐ Ausencia de documentación oficial
☒ Acceso a usuario no autorizados
Incidentes con Sistemas/Software
☒ Falla de Sistemas principales

☒ Falla del Software
☒ Falla de en las herramientas de MS Office
☐ Corrupción/Falla de Software de Maquina Virtuales
☐ Corrupción de Base de Datos SQL Server
☐ Corrupción de Base de Datos Oracle
☐ Corrupción de Base de Respaldos Datos SQL Server
☐ Corrupción de Base de Respaldos Datos Oracle
☐ Falta/Falla de Respaldos de los sistemas principales
☐ Falta/Falla de Respaldos de Maquinas Virtuales
☐ Falta/Falla de Respaldos de Bases de Datos
Incidentes con Equipos Tecnológicos
☒ Falla/Daño en los smartphones
☒ Falla/Daño en Impresoras Móviles
☒ Falla/Daño en Impresoras Fijas
☒ Falla/Daño en Físico Tablets
☒ Falla/Daño en Físico en PDA
☒ Falla/Daño Físico en Computadora
☐ Falla en la Infraestructura interna de Red
Incidentes con Servicios Externos
☒ Falla de Paquete de Servicios de Internet Móvil
☒ Falla de Paquete de Servicios de Internet Corporativo
☐ Falla con Servicios de Proveedor de Almacenamiento en la Nube
Otros incidentes especifique

3. **Indique la frecuencia de ocurrencia de incidentes relacionados con los dispositivos y/o sistemas tecnológicos.**

Criterios de Frecuencia de Ocurrencia de incidentes	
Alta	El evento se presenta más de 4 veces al mes
Media	El evento probablemente se presente 2 veces al mes
Muy Bajo	El Evento podria ocurrir en cualquier momento en los próximos 3 o 4 meses
Bajo	Nunca se ha presentado el evento

Delincuencia Común	**Muy Baja**	**Baja**	**Media**	**Alta**
Sabotaje (ataque físico y electrónico)	X			
Daños por vandalismo	X			
fraude / Estafa	X			
Robo (físico) (Computadoras, Tablet, Smartphone, PDA)	X			
Robo de información electrónica		X		
Intrusión a Red interna	X			
Virus / Ejecución no autorizado de programas	/			X
Violación a derechos de autor		X		
Desastres Naturales	**Muy Baja**	**Baja**	**Media**	**Alta**
Incendio		X		
Sismos				X
Polvo				X
ventilación inadecuada		X		

Incidentes con Servicios Externos	Muy Baja	Baja	Media	Alta
Falla de Paquete de Servicios de Internet Móvil				X
Falla de Paquete de Servicios de Internet Corporativo	X			
Falla con Servicios de Proveedor de Almacenamiento en la Nube	X			

4. ¿Cuál es la magnitud del daño que pueden provocar estos riesgos?

Criterios de Magnitud de Daño	
Critico	Paralización indefinida de las operaciones de ventas de la compañía El evento podría provocar pérdidas económicas irreversibles para la compañía. El posible cierre de la compañía. Insatisfacción con los clientes mas importantes
Alto	Perdidas Económicas graves (10, 000 C$ a 80,000 C$) Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa Las operaciones de ventas se encuentran paralizadas más de 2 días
Medio	Insatisfacción con los clientes más importantes Efecto negativo en la imagen de la empresa Perdidas Económicas moderadas(1000 C$ a 10,000 C$) Las operaciones de ventas se encuentran paralizadas durante medio día
Bajo	No hay efectos negativos para la compañía Las operaciones de ventas no se ven afectadas

Delincuencia Común	Critico	Alto	Medio	Bajo
Sabotaje (ataque físico y electrónico)	X			
Daños por vandalismo				X
fraude / Estafa				X
Robo (físico) (Computadoras, Tablet, Smartphone, PDA)				X
Robo de información electrónica			X	
Intrusión a Red interna	X			
Virus / Ejecución no autorizado de programas			X	
Violación a derechos de autor				X
Desastres Naturales	**Critico**	**Alto**	**Medio**	**Bajo**
Incendio	X			
Sismos			X	
Polvo				X
Ventilación inadecuada				X
Falla de corriente eléctrica			X	
Responsabilidad de Usuario Final y decisiones institucionales	**Critico**	**Alto**	**Medio**	**Bajo**
Falta de inducción, capacitación y sensibilización sobre el uso herramientas tecnológicas				X
Mal manejo de sistemas y herramientas			X	
Utilización de programas no autorizados / software 'pirateado'				X
Falta de pruebas de software nuevo con datos productivos			X	
Pruebas del Software				X
Pérdida de datos			X	
Manejo inadecuado de datos críticos (codificar, borrar, etc.)			X	
Unidades portables con información sin cifrado				X
Transmisión no cifrada de datos críticos				X
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)			X	
Compartir contraseñas o permisos a terceros no autorizados			X	
Transmisión de contraseñas por medios no oficiales				X
Exposición o extravío de equipo, unidades de almacenamiento, etc			X	
Sobrepasar autoridades				X

Falla de fluido eléctrico				X
Responsabilidad de Usuario Final y decisiones institucionales	**Muy Baja**	**Baja**	**Media**	**Alta**
Falta de inducción, capacitación y sensibilización el uso herramientas tecnológicas		X		
Mal manejo de sistemas y herramientas				X
Utilización de programas no autorizados / software 'pirateado'				X
Falta de pruebas de software nuevo con datos productivos		X		
Pruebas del Software		X		
Pérdida de datos			X	
Manejo inadecuado de datos críticos (codificar, borrar, etc.)		X		
Unidades portables con información sin cifrado				X
Transmisión no cifrada de datos críticos		X		
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)				X
Compartir contraseñas o permisos a terceros no autorizados				X
Transmisión de contraseñas por medios no oficiales			X	
Exposición o extravío de equipo, unidades de almacenamiento	X			
Sobrepasar autoridades			X	
Falta de definición de perfil, privilegios y restricciones del personal		X		
Falta de mantenimiento físico (proceso, repuestos e insumos)		X		
Falta de actualización de software (proceso y recursos)	X			
Fallas en permisos de usuarios (acceso a archivos)		X		
Acceso electrónico no autorizado a sistemas externos	X			
Acceso electrónico no autorizado a sistemas internos	X			
Red cableada expuesta para el acceso no autorizado		X		
Red inalámbrica expuesta al acceso no autorizado		X		
Dependencia a servicio técnico externo	X			
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)		X		
Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control		X		
Ausencia de documentación oficial		X		
Acceso a usuario no autorizados			X	
Incidentes con Sistemas/Software	**Muy Baja**	**Baja**	**Media**	**Alta**
Falla de Sistemas principales	X			
Falla del Software			X	
Falla de en las herramientas de MS Office			X	
Corrupción/Falla de Software de Maquina Virtuales	X			
Corrupción de Base de Datos SQL Server	X			
Corrupción de Base de Datos Oracle	X			
Corrupción de Base de Respaldos Datos SQL Server	X			
Corrupción de Base de Respaldos Datos Oracle	X			
Falta/Falla de Respaldos de los sistemas principales		X		
Falta/Falla de Respaldos de Maquinas Virtuales		X		
Falta/Falla de Respaldos de Bases de Datos		X		
Incidentes con Equipos Tecnológicos	**Muy Baja**	**Baja**	**Media**	**Alta**
Falla/Daño en los smartphones				X
Falla/Daño en Impresoras Móviles				X
Falla/Daño en Impresoras Fijas	X			
Falla/Daño en Físico Tablets				X
Falla/Daño en Físico en PDA				X
Falla/Daño Físico en Computadora			X	
Falla en la Infraestructura interna de Red	X			

Falta de definición de perfil, privilegios y restricciones del personal				X
Falta de mantenimiento físico (proceso, repuestos e insumos)				X
Falta de actualización de software (proceso y recursos)				X
Fallas en permisos de usuarios (acceso a archivos)				X
Acceso electrónico no autorizado a sistemas externos				X
Acceso electrónico no autorizado a sistemas internos				X
Red cableada expuesta para el acceso no autorizado				X
Red inalámbrica expuesta al acceso no autorizado				X
Dependencia a servicio técnico externo				X
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)				X
Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control				X
Ausencia de documentación oficial				X
Acceso a usuario no autorizados				X
Incidentes con Sistemas/Software	**Critico**	**Alto**	**Medio**	**Bajo**
Falla de Sistemas principales	X			
Falla del Software				X
Falla de en las herramientas de MS Office				X
Corrupción/Falla de Software de Maquina Virtuales		X		
Corrupción de Base de Datos SQL Server	X			
Corrupción de Base de Datos Oracle	X			
Corrupción de Base de Respaldos Datos SQL Server				X
Corrupción de Base de Respaldos Datos Oracle				X
Falta/Falla de Respaldos de los sistemas principales				X
Falta/Falla de Respaldos de Maquinas Virtuales				X
Falta/Falla de Respaldos de Bases de Datos				X
Incidentes con Equipos Tecnológicos	**Critico**	**Alto**	**Medio**	**Bajo**
Falla/Daño en los smartphones			X	
Falla/Daño en Impresoras Móviles				X
Falla/Daño en Impresoras Fijas			X	
Falla/Daño en Físico Tablets				X
Falla/Daño en Físico en PDA				X
Falla/Daño Físico en Computadora			X	
Falla en la Infraestructura interna de Red	X			
Incidentes con Servicios Externos	**Critico**	**Alto**	**Medio**	**Bajo**
Falla de Paquete de Servicios de Internet Móvil				X
Falla de Paquete de Servicios de Internet Corporativo				X
Falla con Servicios de Proveedor de Almacenamiento en la Nube	X			

ANEXO 5. PROYECTO COMO CONSULTORIA EXTERNA

Para llevar a cabo la realización del proyecto los profesionales propuestos para colaborar en el desarrollo, deben de conocer las Normativas más utilizadas para evaluar las tecnologías de información, tales como ERM, CobiT, ITIL, BS 7799, ISO series 31000, 27000

Personal que participara en el proyecto

Líder del proyecto: es el responsable de planificar y ejecutar la gestión de riesgos; lo que implica las siguientes responsabilidades:

- Definir los diferentes roles en la gestión de riesgos y asignarlos a las personas implicadas. En los proyectos de mayor tamaño, esto puede incluir asignar un director de gestión de riesgos, aunque en proyectos menor esta función la asume el propio director del proyecto o algún miembro del equipo.
- Dirigir y seguir el proceso de identificación y gestión de riesgos.
- Integrar la gestión de riesgos en el plan de gestión de proyecto.
- Resolución de conflictos y dar continuidad al proceso
- Presentar el producto final

El líder de proyecto deberá tener el siguiente perfil profesional: Consultor dedicado a la elaboración de Evaluaciones de Riesgo Tecnológico y Operacional e implementación de Planes de Contingencia de TI y Planes de Continuidad de Negocio, Políticas de seguridad de TI en Entidades Financieras, Aseguradoras y Empresas Distribuidoras de productos masivos, trabajos de Administración de Riesgo.

Miembro del equipo de proyecto: el miembro del equipo de proyecto su responsabilidad es llevar a cabo las tareas designadas por el líder de proyecto:

- Aportar los conocimientos técnicos y experiencia para soportar en la identificación y evaluación de riesgos, y en la definición de acciones.
- Dar soporte y participar en la implementación de las acciones definidas.
- Evaluar y reportar la evolución de las acciones y el riesgo a lo largo del proyecto
- Crear cuestionarios
- Realizar las entrevistas
- Procesar la información concerniente a los riesgos encontrados
- Construir la matriz de evaluación de riesgos
- Brindar las recomendaciones
- Capacitar al personal en el uso de las herramientas de evaluación de riesgos.

El equipo de trabajo designado para tal labor, será el siguiente: Líder de Proyecto y 2 miembros de equipo de trabajo.

Para el desarrollo del proyecto, es importante considerar que se requiere la participación e involucramiento de las áreas interesadas, desde los niveles de Gerencia de tecnologías, jefes de área, hasta los principales colaboradores de las diferentes áreas.

Duración de ejecución del proyecto

Se estima que la duración del proyecto puede abarcar las 2 semanas con el equipo de trabajo estimado, trabajando 5 días laborales en la jornada laboral normal de 8 horas, dando un total de 80 horas de trabajo.

Honorarios profesionales y gastos

Para estimar los honorarios profesionales se parte de las actividades que se requiere ejecutar para lograr los objetivos; del tiempo estimado que debe invertirse para llevarlas a cabo y la formación, habilidades y destrezas de los consultores que las

ejecutarán, al mismo tiempo se incluyen los gastos administrativos que con lleva el proyecto.

Tabla 15 Costo asociados con el proyecto

Rol	Cantidad Personal	Horas	Costo por hora de trabajo	Costo Total
Lider de Proyecto	1	30	$40.00	$1200.00
Miembros de equipo de trabajo	2	50	$25.00	$2500.00
	Costos administrativos	**Cantidad**	**Costo**	
	Resma Papel	2	$20.00	$40.00
	Cartuchos de impresión	2	$25.00	$50.00
	Costo de transporte	1	$200.00	$200.00
	Costo de alimetanción	1	$300.00	$300.00
			Costo total	**$4290.00**

Así mismo, la empresa dotará al equipo de trabajo de espacio físico si es necesario, sala de reuniones, archivos seguros, comunicaciones, acceso a Internet y autorización para ingresar a las instalaciones en horas laborales normales.